

Exhibit 1

[SUBSCRIBE](#)

BACKCHANNEL 07.10.18 01:29 PM

A LANDMARK LEGAL SHIFT OPENS PANDORA'S BOX FOR DIY GUNS

Cody Wilson makes digital files that let anyone 3-D print untraceable guns. The government tried to stop him. He sued—and won.

BY ANDY GREENBERG

FIVE YEARS AGO, 25-year-old radical libertarian Cody Wilson stood on a remote central Texas gun range and pulled the trigger on the world's first [fully 3-D-printed gun](#). When, to his relief, his plastic invention fired a .380-caliber bullet into a berm of dirt without jamming or exploding in

his hands, he drove back to Austin and uploaded the blueprints for the pistol to his website, Defcad.com.

He'd launched the site months earlier along with an anarchist video manifesto, declaring that gun control would never be the same in an era when anyone can download and print their own firearm with a few clicks. In the days after that first test-firing, his gun was downloaded more than 100,000 times. Wilson made the decision to go all in on the project, dropping out of law school at the University of Texas, as if to confirm his belief that technology supersedes law.

Cody Wilson, the founder of Defense Distributed, plans to create the world's largest repository of digital gun files. MICHELLE GROSKOPF

The law caught up. Less than a week later, Wilson received a letter from the US State Department demanding that he take down his printable-gun blueprints or face prosecution for violating federal export controls.

Under an obscure set of US regulations known as the International Trade in Arms Regulations (ITAR), Wilson was accused of exporting weapons without a license, just as if he'd shipped his plastic gun to Mexico rather than put a digital version of it on the internet. He took Defcad.com offline, but his lawyer warned him that he still potentially faced millions of dollars in fines and years in prison simply for having made the file available to overseas downloaders for a few days. "I thought my life was over," Wilson says.

Instead, Wilson has spent the last years on an unlikely project for an anarchist: Not simply defying or skirting the law but taking it to court and changing it. In doing so, he has now not only defeated a legal threat to his own highly controversial gunsmithing project. He may have also unlocked a new era of digital DIY gunmaking that further undermines gun

control across the United States and the world—another step toward
Wilson's imagined future where anyone can make a deadly weapon at
home with no government oversight.

Two months ago, the Department of Justice quietly offered Wilson a settlement to end a lawsuit he and a group of co-plaintiffs have pursued since 2015 against the United States government. Wilson and his team of lawyers focused their legal argument on a free speech claim: They pointed out that by forbidding Wilson from posting his 3-D-printable data, the State Department was not only violating his right to bear arms but his right to freely share information. By blurring the line between a gun and a digital file, Wilson had also successfully blurred the lines between the Second Amendment and the First.

"If code is speech, the constitutional contradictions are evident," Wilson explained to WIRED when he first launched the lawsuit in 2015. "So what if this code is a gun?"

The Department of Justice's surprising settlement, confirmed in court documents earlier this month, essentially surrenders to that argument. It promises to change the export control rules surrounding any firearm below .50 caliber—with a few exceptions like fully automatic weapons and rare gun designs that use caseless ammunition—and move their regulation to the Commerce Department, which won't try to police technical data about the guns posted on the public internet. In the meantime, it gives Wilson a unique license to publish data about those weapons anywhere he chooses.

"I consider it a truly grand thing," Wilson says. "It will be an irrevocable part of political life that guns are downloadable, and we helped to do that."

Now Wilson is making up for lost time. Later this month, he and the nonprofit he founded, Defense Distributed, are relaunching their website Defcad.com as a repository of firearm blueprints they've been privately

creating and collecting, from the original one-shot 3-D-printable pistol he fired in 2013 to AR-15 frames and more exotic DIY semi-automatic weapons. The relaunched site will be open to user contributions, too; Wilson hopes it will soon serve as a searchable, user-generated database of practically any firearm imaginable.

All of that will be available to anyone anywhere in the world with an uncensored internet connection, to download, alter, remix, and fabricate into lethal weapons with tools like 3-D printers and computer-controlled milling machines. “We’re doing the encyclopedic work of collecting this data and putting it into the commons,” Wilson says. “What’s about to happen is a Cambrian explosion of the digital content related to firearms.” He intends that database, and the inexorable evolution of homemade weapons it helps make possible, to serve as a kind of bulwark

against all future gun control, demonstrating its futility by making access to weapons as ubiquitous as the internet.

Of course, that mission seemed more relevant when Wilson first began dreaming it up, before a political party with no will to rein in America's gun death epidemic held control of Congress, the White House, and likely soon the Supreme Court. But Wilson still sees Defcad as an answer to the resurgent gun control movement that has emerged in the wake of the Parkland, Florida, high school shooting that left 17 students dead in February.

The potential for his new site, if it functions as Wilson hopes, would also go well beyond even the average Trump supporter's taste in gun rights. The culture of homemade, unregulated guns it fosters could make firearms available to even those people who practically every American agrees shouldn't possess them: felons, minors, and the mentally ill. The result could be more cases like that of John Zawahiri, an emotionally disturbed 25-year-old who went on a shooting spree in Santa Monica, California, with a homemade AR-15 in 2015, killing five people, or Kevin Neal, a Northern California man who killed five people with AR-15-style rifles—some of which were homemade—last November.

"This should alarm everyone," says Po Murray, chairwoman of Newtown Action Alliance, a Connecticut-focused gun control group created in the wake of the mass shooting at Sandy Hook Elementary School in 2013. "We're passing laws in Connecticut and other states to make sure these weapons of war aren't getting into the hands of dangerous people. They're working in the opposite direction."

When reporters and critics have repeatedly pointed out those potential consequences of Wilson's work over the last five years, he has argued that he's not seeking to arm criminals or the insane or to cause the deaths of innocents. But nor is he moved enough by those possibilities to give up

what he hopes could be, in a new era of digital fabrication, the winning move in the battle over access to guns.

With his new legal victory and the Pandora's box of DIY weapons it opens, Wilson says he's finally fulfilling that mission. "All this Parkland stuff, the students, all these dreams of 'common sense gun reforms'? No. The internet will serve guns, the gun is downloadable." Wilson says now. "No amount of petitions or die-ins or anything else can change that."

DEFENSE DISTRIBUTED OPERATES out of an unadorned building in a north Austin industrial park, behind two black-mirrored doors marked only with the circled letters "DD" scrawled by someone's finger in the dust. In the machine shop inside, amid piles of aluminum shavings, a linebacker-sized, friendly engineer named Jeff Winkleman is walking me through the painstaking process of turning a gun into a collection of numbers.

Winkleman has placed the lower receiver of an AR-15, the component that serves as the core frame of the rifle, on a granite table that's been calibrated to be perfectly flat to one ten-thousandth of an inch. Then he places a Mitutoyo height gauge—a thin metal probe that slides up and down on a tall metal stand and measures vertical distances—next to it, poking one edge of the frame with its probe to get a baseline reading of its position. "This is where we get down to the nitty gritty," Winkleman says. "Or, as we call it, the gnat's ass."

Winkleman then slowly rotates the gauge's rotary handle to move its probe down to the edge of a tiny hole on the side of the gun's frame. After a couple careful taps, the tool's display reads 0.4775 inches. He has just measured a single line—one of the countless dimensions that define the shape of any of the dozens of component of an AR-15—with four decimal places of accuracy. Winkleman's job at Defense Distributed now is to repeat that process again and again, integrating that number, along with every measurement of every nook, cranny, surface, hole, lip, and ridge of

a rifle, into a CAD model he's assembling on a computer behind him, and then to repeat that obsessively comprehensive model-building for as many guns as possible.

That a digital fabrication company has opted for this absurdly manual process might seem counterintuitive. But Winkleman insists that the analog measurements, while infinitely slower than modern tools like laser scanners, produce a far more accurate model—a kind of gold master for any future replications or alterations of that weapon. "We're trying to set a precedent here," Winkleman says. "When we say something is true, you absolutely know it's true."

One room over, Wilson shows me the most impressive new toy in the group's digitization toolkit, one that arrived just three days earlier: A room-sized analog artifact known as an optical comparator. The device, which he bought used for \$32,000, resembles a kind of massive cartoon X-ray scanner.

Defense Distributed's optical comparator, a room-sized machine the group is using to convert physical guns to collections of digital measurements. MICHELLE GROSKOPF

Wilson places the body of an AR-9 rifle on a pedestal on the right side of the machine. Two mercury lamps project neon green beams of light onto the frame from either side. A lens behind it bends that light within the machine and then projects it onto a 30-inch screen at up to 100X magnification. From that screen's mercury glow, the operator can map out points to calculate the gun's geometry with microscopic fidelity. Wilson flips through higher magnification lenses, then focuses on a series of tiny ridges of the frame until the remnants of their machining look like the brush strokes of Chinese calligraphy. "Zoom in, zoom in, enhance" Wilson jokes.

SUBSCRIBE

Wilson's first controversial innovation was to demonstrate how digital files could be converted to physical, deadly weapons.

MICHELLE GROSKOPF

He now sees an opportunity to cripple gun control with the opposite tactic: digitizing as many weapons as possible and making the files available to gunsmiths.

MICHELLE GROSKOPF

Turning physical guns into digital files, instead of vice-versa, is a new trick for Defense Distributed. While Wilson's organization first gained notoriety for its invention of the first 3-D printable gun, what it called the Liberator, it has since largely moved past 3-D printing. Most of the company's operations are now focused on its core business: making and selling a consumer-grade computer-controlled milling machine known as the Ghost Gunner, designed to allow its owner to carve gun parts out of far more durable aluminum. In the largest room of Defense Distributed's headquarters, half a dozen millennial staffers with beards and close-cropped hair—all resembling Cody Wilson, in other words—are busy building those mills in an assembly line, each machine capable of skirting all federal gun control to churn out untraceable metal glocks and semiautomatic rifles en masse.

The staff of Defense Distributed: part startup, part advocacy group, part armed insurgency.

MICHELLE GROSKOPF

For now, those mills produce only a few different gun frames for firearms, including the AR-15 and 1911 handguns. But Defense Distributed's engineers imagine a future where their milling machine and other digital fabrication tools—such as consumer-grade aluminum-sintering 3-D printers that can print objects in metal—can make practically any digital gun component materialize in someone's garage.

SUBSCRIBE

Most of Defense Distributed's staff work on the group's central source of revenue: building gun-making computer controlled milling machines called the Ghost Gunner

MICHELLE GROSKOPF

A Ghost Gunner can finish an AR-15 lower receiver, the central part of the rifle's frame, in a few hours. Defense Distributed has sold close to 6,000 of the machines.

MICHELLE GROSKOPF

In the meantime, selling Ghost Gunners has been a lucrative business. Defense Distributed has sold roughly 6,000 of the desktop devices to DIY gun enthusiasts across the country, mostly for \$1,675 each, netting millions in profit. The company employs 15 people and is already outgrowing its North Austin headquarters. But Wilson says he's never been interested in money or building a startup for its own sake. He now claims that the entire venture was created with a singular goal: to raise enough money to wage his legal war against the US State Department.

AFTER HIS LAWYERS originally told him in 2013 that his case against the government was hopeless, Wilson fired them and hired two new ones with expertise in export control and both Second and First-Amendment law. Matthew Goldstein, Wilson's lawyer who is focused on ITAR, says he was immediately convinced of the merits of Wilson's position. "This is the case you'd bring out in a law school course as an unconstitutional law," Goldstein says. "It ticks all the check boxes of what violates the First Amendment."

When Wilson's company teamed up with the Second Amendment Foundation and brought their lawsuit to a Texas District court in 2015, they were supported by a collection of amicus briefs from a shockingly broad coalition: Arguments in their favor were submitted by not only the libertarian Cato Institute, the gun-rights-focused Madison Society, and 15

Republican members of Congress but also the Electronic Frontier SUBSCRIBE Foundation and the Reporters Committee for Freedom of the Press.

When the judge in the case nonetheless rejected Defense Distributed's request for a preliminary injunction that would have immediately allowed it to continue publishing gun files, the company appealed, and lost. But as the case proceeded toward a ruling on Defense Distributed's first amendment argument, the government surprised the plaintiffs by suddenly offering them a settlement with essentially everything they wanted. It even pays back \$40,000 of their court costs and paperwork fees. (Wilson says that's still only about 10 percent of the \$400,000 that the plaintiffs spent.)

Goldstein says the settlement may have had as much to do with ITAR reforms begun during the Obama administration as with the gun-friendly Trump administration that took over the case. But he doesn't rule out that a new regime may have helped tip the balance in the plaintiffs' favor. "There's different management at the helm of this agency," Goldstein says. "You can draw your own conclusions." Both the Department of Justice and the State Department declined to comment on the outcome of the case.

With the rule change their win entails, Defense Distributed has removed a legal threat to not only its project but an entire online community of DIY gunmakers. Sites like GrabCAD and FossCad already host hundreds of gun designs, from Defense Distributed's Liberator pistol to printable revolvers and even semiautomatic weapons. "There's a lot of satisfaction in doing things yourself, and it's also a way of expressing support for the Second Amendment," explains one prolific FossCad contributor, a West Virginian serial inventor of 3-D-printable semiautomatics who goes by the pseudonym Derwood. "I'm a conservative. I support all the amendments."

But until now, Derwood and practically every other participant on those platforms risked prosecution for violating export controls, whether they knew it or not. Though enforcement has been rare against anyone less vocal and visible than Wilson, many online gunsmiths have nonetheless obscured their identities for that reason. With the more open and intentional database of gun files that Defcad represents, Wilson believes he can create a collection of files that's both more comprehensive and more refined, with higher accuracy, more detailed models for every component, giving machinists all the data they need to make or remix them. "This is the stuff that's necessary for the creative work to come," Wilson says.

In all of this, Wilson sees history repeating itself: He points to the so-called Crypto Wars of the 1990s. After programmer Philip Zimmermann in 1991 released PGP, the world's first free encryption program that anyone could use to thwart surveillance, he too was threatened with an indictment for violating export restrictions. Encryption software was, at the time, treated as a munition and placed on the same prohibited export control list as guns and missiles. Only after a fellow cryptographer, Daniel Bernstein, sued the government with the same free-speech argument Wilson would use 20 years later did the government drop its investigation of Zimmermann and spare him from prison.

"This is a specter of the old thing again," Wilson says. "What we were actually fighting about in court was a core crypto-war problem." And following that analogy, Wilson argues, his legal win means gun blueprints can now spread as widely as encryption has since that earlier legal fight: After all, encryption has now grown from an underground curiosity to a commodity integrated into apps, browsers, and websites running on billions of computers and phones across the globe.

But Zimmermann takes issue with the analogy—on ethical if not legal grounds. This time, he points out, the First Amendment-protected data that was legally treated as a weapon actually *is* a weapon. "Encryption is

a defense technology with humanitarian uses," Zimmermann says. "Guns are only used for killing."

"Arguing that they're the same because they're both made of bits isn't quite persuasive for me," Zimmermann says. "Bits can kill."

AFTER A TOUR of the machine shop, Wilson leads me away from the industrial roar of its milling machines, out the building's black-mirrored-glass doors and through a grassy patch to its back entrance. Inside is a far quieter scene: A large, high-ceilinged, dimly fluorescent-lit warehouse space filled with half a dozen rows of gray metal shelves, mostly covered in a seemingly random collection of books, from *The Decline and Fall of the Roman Empire* to *Hunger Games*. He proudly points out that it includes the entire catalog of Penguin Classics and the entire Criterion Collection, close to 900 Blu-rays. This, he tells me, will be the library.

And why is Defense Distributed building a library? Wilson, who cites Baudrillard, Foucault, or Nietzsche at least once in practically any conversation, certainly doesn't mind the patina of erudition it lends to what is essentially a modern-day gun-running operation. But as usual, he has an ulterior motive: If he can get this room certified as an actual, official public library, he'll unlock another giant collection of existing firearm data. The US military maintains records of thousands of the specs for thousands of firearms in technical manuals, stored on reels and reels of microfiche cassettes. But only federally approved libraries can access them. By building a library, complete with an actual microfiche viewer in one corner, Wilson is angling to access the US military's entire public archive of gun data, which he eventually hopes to digitize and include on Defcad.com, too.

To exploit a technical loophole that gives him access to military weapons files, Cody Wilson is also building a library. He proudly notes it will include the entire Criterion Collection on Blu-ray.

MICHELLE GROSKOPF

"Ninety percent of the technical data is already out there. This is a huge part of our overall digital intake strategy," Wilson says. "Hipsters will come here and check out movies, independent of its actual purpose, which is a stargate for absorbing ancient army technical materials."

Browsing that movie collection, I nearly trip over something large and hard. I look down and find a granite tombstone with the words AMERICAN GUN CONTROL engraved on it. Wilson explains he has a plan to embed it in the dirt under a tree outside when he gets around to it. "It's maybe a little on the nose, but I think you get where I'm going with it," he says.

Wilson plans to bury this tombstone by his library's entrance. "It's maybe a little on the nose," he admits.

MICHELLE GROSKOPF

Wilson's library will serve a more straightforward purpose, too: In one corner stands a server rack that will host Defcad's website and backend database. He doesn't trust any hosting company to hold his controversial files. And he likes the optics of storing his crown jewels in a library, should any reversal of his legal fortunes result in a raid. "If you want to come get it, you have to attack a library," he says.

On that subject, he has something else to show me. Wilson pulls out a small embroidered badge. It depicts a red, dismembered arm on a white background. The arm's hand grips a curved sword, with blood dripping from it. The symbol, Wilson explains, once flew on a flag above the Goliad Fort in South Texas. In Texas' revolution against Mexico in the 1830s,

Goliad's fort was taken by the Mexican government and became the site of a massacre of 400 American prisoners of war, one that's far less widely remembered than the Alamo.

Wilson recently ordered a full-size flag with the sword-wielding bloody arm. He wants to make it a new symbol for his group. His interest in the icon, he explains, dates back to the 2016 election, when he was convinced Hillary Clinton was set to become the president and lead a massive crackdown on firearms.

The flag of Goliad, which Wilson has adopted as a new symbol for his group. He suggests you interpret it as you will. MICHELLE GROSCHOPF

If that happened, as Wilson tells it, he was ready to launch his Defcad repository, regardless of the outcome of his lawsuit, and then defend it in an armed standoff. "I'd call a militia out to defend the server, Bundy-style," Wilson says calmly, in the first overt mention of planned armed violence I've ever heard him make. "Our only option was to build an infrastructure where we had one final suicidal mission, where we dumped everything into the internet," Wilson says. "Goliad became an inspirational thing for me."

Now, of course, everything has changed. But Wilson says the Goliad flag still resonates with him. And what does that bloody arm symbol mean to him now, in the era where Donald Trump is president and the law has surrendered to his will? Wilson declines to say, explaining that he would rather leave the mystery of its abstraction intact and open to interpretation.

But it doesn't take a degree in semiotics to see how the Goliad flag suits Defense Distributed. It reads like the logical escalation of the NRA's "cold

dead hands” slogan of the last century. In fact, it may be the perfect symbol not just for Defense Distributed’s mission but for the country that produced it, where firearms result in tens of thousands of deaths a year—vastly more than any other developed nation in the world—yet groups like Wilson’s continue to make more progress in undermining gun control than lawmakers do in advancing it. It’s a flag that represents the essence of violent extremist ideology: An arm that, long after blood is spilled, refuses to let go. Instead, it only tightens its grip on its weapon, as a matter of principle, forever.

More Great WIRED Stories

- Our own Andy Greenberg made an untraceable AR-15 in the office, [and it was easy](#)
- This \$1200 machine lets anyone [make a metal gun at home](#)
- This giant invasive flower can give you [third-degree burns](#)
- The Pentagon’s dream team of [tech-savvy soldiers](#)
- PHOTO ESSAY: The annual super-celebration in Superman’s [real-world home](#)
- It’s time you learned about [quantum computing](#)
- Boeing’s proposed hypersonic plane is [really really fast](#)
- Get even more of our inside scoops with our weekly [Backchannel newsletter](#)

Corrected 7/10/2018 2:30 EST to note that the first 3-D printed gun used .380-caliber ammunition, not .223-caliber.*

SUBSCRIBE

RELATED VIDEO

CULTURE

I Made an Untraceable AR-15 'Ghost Gun' In My Office

WIRED senior writer Andy Greenberg puts new homemade gunsmithing tools to the test as he tries three ways of building an untraceable AR-15 semi-automatic rifle---a so-called "ghost gun"---while skirting all gun control laws.

[VIEW COMMENTS](#)

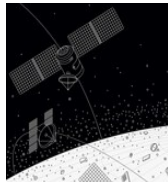
SPONSORED STORIES

POWERED BY OUTBRAIN



DANIEL
DUANE

How the
Secrets
of
Called into
the Day



GARRETT M.
GRAFF

The New
Arms Race
Threatening



LAUREN
SMILEY

The Mission
to Build the
Ultimate
Support for



ADAM
ROGERS

Big Tech
Tackles the
Problem
With
Homemade



JASON
PARHAM

How Oprah's
Network
Finally
Found its
Voice

MORE BACKCHANNEL

SUBSCRIBE

FOR ALL TO SEEK

A Deadly Hunt for Hidden Treasure Spawns an Online Mystery

DAVID KUSHNER

BACKCHANNEL

Inside the 23-Dimensional World of Your Car's Paint Job

ADAM ROGERS

SUBSCRIBE

PIVOT

The Political Education of Silicon Valley

STEVEN JOHNSON

PARENTING

One Young Boy's Magnificent Obsession With Fans

CATHY ALTER

SUBSCRIBE

BACKCHANNEL

Shadow Politics: Meet the Digital Sleuth Exposing Fake News

ISSIE LAPOWSKY

TOMATO, TOMORROW

Crispr Can Speed Up Nature—and Change How We Grow Food

STEPHEN S. HALL

GET BACKCHANNEL'S NEWSLETTER

We publish our biggest stories on Wednesdays. Be the first to know.

SUBSCRIBE

**FOLLOW US
ON FACEBOOK**



Backchannel is moving to Wired! Here's what that means:

<http://trib.al/Ar1TZSg>
Get Backchannel's latest stories and
live videos.

SUBSCRIBE | ADVERTISE | SITE MAP | PRESS CENTER | FAQ | ACCESSIBILITY HELP |
CUSTOMER CARE | CONTACT US | SECUREDROP | T-SHIRT COLLECTION | NEWSLETTER |
FOLLOW
WIRED STAFF | JOBS | RSS

CNMN Collection

© 2018 Condé Nast. All rights reserved.

Use of and/or registration on any portion of this site constitutes acceptance of our User Agreement (updated 5/25/18) and Privacy Policy and Cookie Statement (updated 5/25/18). Your California Privacy Rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast. Ad Choices.

Exhibit 2

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON**

STATE OF WASHINGTON; STATE OF
CONNECTICUT; STATE OF MARYLAND;
STATE OF NEW JERSEY; STATE OF NEW
YORK; STATE OF OREGON;
COMMONWEALTH OF
MASSACHUSETTS; COMMONWEALTH
OF PENNSYLVANIA; and DISTRICT OF
COLUMBIA

Plaintiffs,

v.

UNITED STATES DEPARTMENT OF
STATE; MICHAEL R. POMPEO, in his
official capacity as Secretary of State;
DIRECTORATE OF DEFENSE TRADE
CONTROLS; MIKE MILLER, in his official
capacity as Acting Deputy Assistant Secretary
of Defense Trade Controls; SARAH
HEIDEMA, in her official capacity as Director
of Policy, Office of Defense Trade Controls
Policy; DEFENSE DISTRIBUTED; SECOND
AMENDMENT FOUNDATION, INC; and
CONN WILLIAMSON;

Defendants.

NO.

DECLARATION OF
MITZI JOHANKNECHT
IN SUPPORT OF PLAINTIFF'S
MOTION FOR TRO AND
PRELIMINARY INJUNCTION

Noting Date: August __, 2018

I, Mitzi Johanknecht, declare as follows:

1. I am over the age of 18 and have personal knowledge of all the facts stated herein.
2. I have been the Sheriff of King County, Washington since January 1, 2018.
3. I have been a law enforcement officer for 33 years with the King County Sheriff's

Office (KCSO). During my time as a law enforcement officer, I worked my way up the ranks
from deputy and have served in leadership roles in every division and location in the KCSO. As

1 the Sheriff, I oversee a staff of 1,200 employees who are responsible for the public safety of
 2 approximately 2.2 million people who live in King County, plus thousands of others who transit
 3 to and through the county on a daily basis.

4 4. As a law enforcement officer, I am very familiar with firearms. I have carried a
 5 gun as part of my job for the last 33 years, have received instruction on a variety of weapons
 6 including pistols and long guns, and have personally witnessed the damage that guns can do to
 7 the human body if guns fall into the wrong hands.

8 5. I am also familiar with Washington's gun-safety laws, which prohibit certain
 9 categories of persons from buying or possessing firearms. This group includes minors, persons
 10 convicted of violent felonies, persons under the supervision of the Department of Corrections,
 11 the mentally ill, and persons subject to a wide variety of protection orders, including domestic
 12 violence, stalking and anti-harassment protection orders.

13 6. Washington's gun laws place a significant amount of responsibility on local law
 14 enforcement. For example, the KCSO handles the vetting and granting of applications for
 15 concealed pistol licenses, firearms dealer licenses, and alien firearms licenses for citizens living
 16 in unincorporated areas of King County, as well as those municipalities for which the KCSO
 17 contracts for law enforcement services. Information about such licensing is available on the
 18 KCSO page of the King County website; for example:

19 <https://kingcounty.gov/depts/sheriff/services/gun.aspx> (last visited July 29, 2017);

20 <https://kingcounty.gov/depts/sheriff/services/firearms-dealers.aspx> (last visited July 29,
 21 2017);

22 <https://kingcounty.gov/depts/sheriff/services/alien-firearms-license.aspx> (last visited
 23 July 29, 2017).

9. As I said above, Washington has a very strong and comprehensive set of gun laws designed to ensure that persons who are ineligible under Washington law from possessing firearms cannot obtain guns. The widespread availability of the technology to print guns—especially nonmetal guns that can pass unseen and unrecognized through metal detectors—greatly increases the likelihood that persons who are ineligible to possess guns will be able to get guns. Such a world would be much more dangerous for the public, and for the deputies at the KCSO whose job it is to protect the public.

I declare under penalty of perjury under the laws of the State of Washington and the United States of America that the foregoing is true and correct.

DATED this 30th day of July, 2018, at SEATTLE, Washington.

Mark Frankendall

Exhibit 3

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON**

STATE OF WASHINGTON; STATE OF
CONNECTICUT; STATE OF MARYLAND;
STATE OF NEW JERSEY; STATE OF NEW
YORK; STATE OF OREGON;
COMMONWEALTH OF
MASSACHUSETTS; COMMONWEALTH
OF PENNSYLVANIA; and DISTRICT OF
COLUMBIA,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF
STATE; MICHAEL R. POMPEO, in his
official capacity as Secretary of State;
DIRECTORATE OF DEFENSE TRADE
CONTROLS; MIKE MILLER, in his official
capacity as Acting Deputy Assistant Secretary
of Defense Trade Controls; SARAH
HEIDEMA, in her official capacity as Director
of Policy, Office of Defense Trade Controls
Policy; DEFENSE DISTRIBUTED; SECOND
AMENDMENT FOUNDATION, INC; and
CONN WILLIAMSON

Defendants.

NO.

DECLARATION OF CARMEN BEST
IN SUPPORT OF PLAINTIFF'S
MOTION FOR TRO AND
PRELIMINARY INJUNCTION

Noting Date: August __, 2018

I, Carmen Best, declare as follows:

1. I am over the age of 18 and have personal knowledge of all the facts stated herein.
2. I am the Chief of the Seattle Police Department. I began serving as interim chief on January 1, 2018, and have been nominated to the permanent position by Mayor Jenny Durkan.
3. I have been a law enforcement officer for 26 years with the Seattle Police Department (SPD). During my time as a law enforcement officer, I worked my way up the ranks

1 from deputy and have served in leadership roles in a wide range of positions with SPD, including
 2 school safety, operations lieutenant, and assistant chief in the criminal investigations bureau. As
 3 the Chief of SPD, I oversee a staff of 1945 personnel who are responsible for the public safety
 4 of approximately 725,000 members of the public in Seattle.

5 4. As a law enforcement officer, I am very familiar with firearms. I have carried a
 6 gun as part of my job for the last 26 years, have received instruction on a variety of guns, and
 7 have personally witnessed the damage that guns can do to the human body if guns fall into the
 8 wrong hands.

9 5. I am also familiar with Washington's gun-safety laws, which prohibit certain
 10 categories of persons from buying or possessing firearms. This group includes minors, persons
 11 convicted of violent felonies, persons under the supervision of the Department of Corrections,
 12 the mentally ill, and persons subject to a wide variety of protection orders, including domestic
 13 violence, stalking and anti-harassment protection orders.

14 6. Washington's gun laws place a significant amount of responsibility on local law
 15 enforcement. For example, SPD is responsible for enforcement of court orders to surrender
 16 firearms; testing and processing firearms recovered as evidence; and conducting investigations,
 17 searches, arrests, and other activities that may result in lawful seizure of a firearm. Information
 18 about these responsibilities is contained in the Seattle Police Department Manual, which is
 19 available at the SPD page of the City of Seattle website:

20 [http://www.seattle.gov/police-manual/title-15---primary-investigation/15215---seizing-
 22 and-releasing-firearms](http://www.seattle.gov/police-manual/title-15---primary-investigation/15215---seizing-

 21 and-releasing-firearms) (last visited July 29, 2018);

23 [http://www.seattle.gov/police-manual/title-7---evidence-and-property/7030---firearms-
 ammunition-and-shell-casings](http://www.seattle.gov/police-manual/title-7---evidence-and-property/7030---firearms-

 24 ammunition-and-shell-casings) (last visited July 29, 2018);

1 [http://www.seattle.gov/police-manual/title-6---arrests-search-and-seizure/6180---](http://www.seattle.gov/police-manual/title-6---arrests-search-and-seizure/6180---searches-general)
2 [searches-general](http://www.seattle.gov/police-manual/title-6---arrests-search-and-seizure/6180---searches-general) (last visited July 29, 2018);
3 [http://www.seattle.gov/police-manual/title-15---primary-investigation/15410---](http://www.seattle.gov/police-manual/title-15---primary-investigation/15410---domestic-violence-investigation)
4 [domestic-violence-investigation](http://www.seattle.gov/police-manual/title-15---primary-investigation/15410---domestic-violence-investigation) (last visited July 29, 2018);
5 [http://www.seattle.gov/police-manual/title-16---patrol-operations/16110---crisis-](http://www.seattle.gov/police-manual/title-16---patrol-operations/16110---crisis-intervention)
6 [intervention](http://www.seattle.gov/police-manual/title-16---patrol-operations/16110---crisis-intervention) (last visited July 29, 2018).

7 7. I understand that technology exists that allows the manufacture of firearms
8 through the use of commercially available 3-D printers. I further understand that this technology
9 would allow someone to “print” or make guns in the privacy of his or her own home or anywhere
10 a 3-D printer is available. The guns made in this manner can be constructed out of metal or
11 plastic; regardless, I understand these “ghost guns” generally bear no identifying serial number
12 or manufacturer’s mark. In addition, I understand that the 3-D printed guns made out of plastic
13 are not detectable by metal detectors used at places such as courthouses and airports.

14 8. I have great concern for public safety if the technology (e.g., software, computer
15 files, computer code) that would allow 3-D printers to be used to print guns would become
16 publicly available, including via the internet. As I said above, Washington has a very strong and
17 comprehensive set of gun laws designed to ensure that persons who are ineligible under
18 Washington law from possessing firearms cannot obtain guns. The widespread availability of
19 the technology to print guns—especially nonmetal guns that can pass unseen and unrecognized
20 through metal detectors—greatly increases the likelihood that persons who are ineligible to
21 possess guns will be able to get guns. Such a world would be much more dangerous for the
22 public, and for the SPD officers whose job it is to protect the public.

1 I declare under penalty of perjury under the laws of the State of Washington and the
2 United States of America that the foregoing is true and correct.

3 DATED this 30th day of July, 2018, at Seattle, Washington.

4
5 Carmen Best
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

Exhibit 4

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, et al.,	§	
Plaintiffs,	§	
	§	
v.	§	No. 1:15-cv-372-RP
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
Defendants.	§	

Exhibit A: Declaration of Lisa V. Aguirre

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

DEFENSE DISTRIBUTED, et al.,	§	
Plaintiffs,	§	
	§	
v.	§	No. 1:15-cv-372-RP
	§	
U.S. DEPARTMENT OF STATE, et al.,	§	
Defendants.	§	

DECLARATION OF LISA V. AGUIRRE

I, Lisa Aguirre, pursuant to 28 U.S.C. § 1746, hereby declare and say as follows:

1. I am the Director of the Office of Defense Trade Controls Management (DTCM), one of four directors within the Directorate of Defense Trade Controls (DDTC), Bureau of Political-Military Affairs at the Department of State. I have held this position since June, 2013. My roles and responsibilities in this position include managing, overseeing or supporting all DDTC activities.
2. Prior to holding my current position, I was Director of the Office of Defense Trade Controls Compliance in DDTC for over three years, during which time I oversaw numerous DDTC activities, including the management and processing of registration applications and registration fee submissions, reviews of export licenses for prohibited parties, the DDTC Company Visit Program (CVP), a program in which State Department officials visit arms exporters or end users to gather information on compliance with the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), and reviews under the

Committee on Foreign Investment in the United States (CFIUS). As Compliance Director, I also oversaw civil enforcement actions and provided support to criminal enforcement matters under ITAR. In these capacities at DDTC, I have become familiar with the application of the AECA and ITAR as part of DDTC's mission and the full range of DDTC activities in support of its mission.

3. Since joining DDTC, first as a contractor in June 2007, and then through appointment to the federal service in July 2008, I have served continuously in defense trade controls roles.
4. This declaration is submitted in support of the opposition to a motion for preliminary injunction to be filed by the official capacity defendants in the above-captioned case. The information contained herein is based on my personal knowledge and on information provided to me in my official capacity.

Directorate of Defense Trade Controls

5. The Directorate of Defense Trade Controls (DDTC) is part of the Department of State's Bureau of Political-Military Affairs (PM), which reports to the Under Secretary for Arms Control and International Security. DDTC controls the export and temporary import and brokering of defense articles and services covered by the United States Munitions List (USML), in accordance with 22 U.S.C. §§ 2778-2780 of the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130).

6. DDTC's mission is to carry out the purposes of the AECA to further world peace and the national security and foreign policy of the United States, including by ensuring that commercial defense exports support key objectives of U.S. national security and foreign policy, including weapons nonproliferation, support for allies, and preservation of human rights. DDTC also seeks to ensure that regulation keeps pace with innovation, that U.S. industry and foreign partners comply with applicable policies and requirements, and that the munitions export process is reliable and predictable. DDTC also serves as a resource to the U.S. government, industry, and foreign counterparts on defense trade matters.
7. As part of its mission, DDTC licenses the export and temporary import and brokering of items subject to the International Traffic in Arms Regulations ("ITAR") and seeks to ensure appropriate compliance with, and enforcement of, these regulations. DDTC also maintains, reviews, and clarifies the U.S. Munitions List (USML), and oversees the Commodity Jurisdiction process.
8. The Office of Defense Trade Controls Policy (DTCP) within the Directorate of Defense Trade Controls oversees the development of policy and guidance related to exports of defense articles and services on the USML and subject to the ITAR and the AECA. DTCP manages the interagency Commodity Jurisdiction process, which determines whether or not certain items are controlled on the USML when questions arise concerning whether or not an item is subject to the licensing jurisdiction of the Department of State. DTCP also prepares all changes to the ITAR, which are published in the Federal Register, manages bilateral defense

trade agreements, such as the United Kingdom and Australia Defense Trade Cooperation Treaties, and provides export control policy and regulatory guidance to exporters, defense manufacturers, and foreign allies and partners.

Statutory and Regulatory Framework

9. The Arms Export Control Act (AECA), Section 38(a)(1) (22 U.S.C. 2778(a)(1)), authorizes the President “in furtherance of world peace and the security and foreign policy of the United States . . . to control the import and the export of defense articles and defense services and to provide foreign policy guidance to persons of the United States involved in the export and import of such articles and services. The President is authorized to designate those items which shall be considered as defense articles and defense services for the purposes of this section and to promulgate regulations for the import and export of such articles and services. The items so designated shall constitute the United States Munitions List.”

- (a) The statutory authority of the President to “promulgate regulations for the import and export of such articles and services” has been delegated to the Secretary of State by Executive Order 13637, § 1(n). This delegation requires that “Designations, including changes in designations, by the Secretary of State of items or categories of items that shall be considered as defense articles and defense services subject to export control under section 38 (22 U.S.C. 2778) shall have the concurrence of the Secretary of Defense.”

(b) The authorities under the AECA delegated to the Secretary of State have been further delegated pursuant to Department of State Delegation of Authority 293-2, *Delegation of Authority by the Secretary of State to Officers of the Department of State and the Administrator of the U.S. Agency for International Development of Authorities under the Foreign Assistance Act of 1961 and Other Related Acts* (Oct. 23, 2011), which delegates to the Under Secretary for Arms Control and International Security “the functions conferred on the Secretary by Executive Order 13637 relating to sales and exports under the Arms Export Control Act (22 U.S.C. 2751 *et seq.*).”

10. The ITAR, 22 C.F.R. Chapter I, Subchapter M, Parts 120-130, as amended, 79 Fed. Reg. 77884 (Dec. 29, 2014), implements the AECA. Section 120.1 of the ITAR sets forth how the ITAR is administered:

(a) Section 38 of the Arms Export Control Act (22 U.S.C. 2778), as amended, authorizes the President to control the export and import of defense articles and defense services. The statutory authority of the President to promulgate regulations with respect to exports of defense articles and defense services is delegated to the Secretary of State by Executive Order 13637. This subchapter implements that authority, as well as other relevant authorities in the Arms Export Control Act (22 U.S.C. 2751 *et seq.*). By virtue of delegations of authority by the Secretary of State, these regulations are primarily administered by the Deputy Assistant Secretary of State for Defense Trade Controls, Bureau of Political-Military Affairs.

11. The ITAR provides what particular activities constitute an export. Section 120.17 defines an “export” to mean:

- (1) Sending or taking a defense article out of the United States in any manner, except by mere travel outside of the United States by a person whose personal knowledge includes technical data; or
- (2) Transferring registration, control or ownership to a foreign person of any aircraft, vessel, or satellite covered by the U.S. Munitions List, whether in the United States or abroad; or
- (3) Disclosing (including oral or visual disclosure) or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government (*e.g.*, diplomatic missions); or
- (4) Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; or
- (5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad.
- (6) A launch vehicle or payload shall not, by reason of the launching of such vehicle, be considered an export for purposes of this subchapter. However, for certain limited purposes (see § 126.1 of this subchapter), the controls of this subchapter may apply to any sale, transfer or proposal to sell or transfer defense articles or defense services.”¹

¹ On June 3, 2015, the Department of State published in the Federal Register a Notice of Proposed Rulemaking (NPRM) proposing revisions to the ITAR. Among other proposed changes, the Department proposed to clarify the definition of “technical data” by

12. Part 121 of the ITAR sets out those “articles, services, and related technical data” that have been designated as defense articles and defense services pursuant to sections 38 and 47(7) of the AECA. These items make up the USML. There are 21 categories on the USML under which a particular item may be designated as a defense article.
13. As relevant to this litigation, under Category I, *Firearms, Close Assault Weapons and Combat Shotguns*, the following items are designated as defense articles:
 - (a) Non-automatic and semi-automatic firearms to caliber .50 inclusive (12.7 mm).
 - (b) Fully automatic firearms to .50 caliber inclusive (12.7 mm).
 - (c) Firearms or other weapons (e.g., insurgency-counterinsurgency, close assault weapons systems) having a special military application regardless of caliber.
 - (d) Combat shotguns. This includes any shotgun with a barrel length less than 18 inches.
 - (e) Silencers, mufflers, sound and flash suppressors for the articles in (a) through (d) of this category and their specifically designed, modified or adapted components and parts.
 - (f) Riflescopes manufactured to military specifications. (See category XII(c) for controls on night sighting devices.)
 - (g) Barrels, cylinders, receivers (frames) or complete breech mechanisms for the articles in paragraphs (a) through (d) of this category.
 - (h) Components, parts, accessories and attachments for the articles in paragraphs (a) through (g) of this category.

specifying that technical data may take the form of, inter alia, CAD files. In addition, to make more explicit the existing control on exports, the Department proposed to add a paragraph specifying that providing technical data on a publicly-accessible network, such as the Internet, is an export because of its inherent accessibility to foreign powers. The Department has requested that interested parties submit comments on these and other elements of the proposed rulemaking between June 3 and August 3, 2015. See Exhibit 7.

- (i) Technical data (as defined in § 120.10 of this subchapter) and defense services (as defined in § 120.9 of this subchapter) directly related to the defense articles described in paragraphs (a) through (h) of this category. Technical data directly related to the manufacture or production of any defense articles described elsewhere in this category that are designated as Significant Military Equipment (SME) shall itself be designated SME.
 - (j) The following interpretations explain and amplify the terms used in this category and throughout this subchapter:
 - (1) A firearm is a weapon not over .50 caliber (12.7 mm) which is designed to expel a projectile by the action of an explosive or which may be readily converted to do so.
 - (2) A rifle is a shoulder firearm which can discharge a bullet through a rifled barrel 16 inches or longer.
 - (3) A carbine is a lightweight shoulder firearm with a barrel under 16 inches in length.
 - (4) A pistol is a hand-operated firearm having a chamber integral with or permanently aligned with the bore.
 - (5) A revolver is a hand-operated firearm with a revolving cylinder containing chambers for individual cartridges.
 - (6) A submachine gun, "machine pistol" or "machine gun" is a firearm originally designed to fire, or capable of being fired, fully automatically by a single pull of the trigger.
14. In addition to the inclusion of "technical data" for Category I defense articles on the USML, there are several other provisions of the ITAR related to "technical data."
- a. Section 120.10 of the ITAR defines "technical data" as "(a)(1) Information, other than software as defined in § 120.10(a)(4) which is required for the design, development, production, manufacture,

assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation[;] (2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List; (3) Information covered by an invention secrecy order; or (4) Software (see § 120.45(f)) directly related to defense articles.² (b)³ The definition in paragraph (a) of this section does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, or information in the public domain as defined in § 120.11 of this subchapter or telemetry data as defined in note 3 to Category XV(f) of part 121 of this subchapter. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.”

- b. Section 120.6 of the ITAR defines a “defense article” as “any item or technical data designated in § 121.1 of this subchapter. This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in § 121.1 of this subchapter. It also includes forgings, castings, and other unfinished products, such as

² This sentence added by 79 FR 61226 (Oct. 10, 2014).

³ Amended by 79 FR 27180 (May 13, 2014, effective Nov. 10, 2014), as corrected by 79 FR 66608 (Nov. 10, 2014).

extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles.⁴ It does not include basic marketing information on function or purpose or general system descriptions.”

- c. Section 120.9 of the ITAR defines a “defense service” as “(1) The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles; (2) The furnishing to foreign persons of any technical data controlled under this subchapter (see § 120.10), whether in the United States or abroad; or (3) Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice. (See also § 124.1.)”
- d. Collectively, the “technical data” provisions serve the purpose of limiting the export of detailed information needed to manufacture, maintain, or operate defense articles controlled on the USML. Such

⁴ This sentence was added to the definition of defense article by 79 FR 61226 (Oct. 10, 2014).

export limitations advance the purposes of the AECA by limiting the ability of foreign powers to design, develop, and produce defense articles in lieu of being able to obtain those articles directly. Absent the inclusion of technical data in the ITAR, the ITAR's limits on arms transfers would be of negligible practical effect because the ITAR would leave unregulated the exportation of the fundamental technology, know-how, blueprints, and other design information sufficient for foreign powers to construct, produce, manufacture, maintain, and operate the very same equipment regulated in its physical form by the ITAR.

15. The ITAR also sets forth the policy on designating and determining how a specific article or service may be designated as a defense article or defense service.
 - a. Pursuant to section 120.3, a particular article or service will be designated as a defense article if it: "(1) Meets the criteria of a defense article or defense service on the U.S. Munitions List; or (2) Provides the equivalent performance capabilities of a defense article on the U.S. Munitions List."
 - b. Section 120.3 also provides that a specific article or service "shall be determined in the future as a defense article or defense service if it provides a critical military or intelligence advantage such that it warrants control" under the ITAR.

c. Section 120.3 also specifies that the “intended use of the article or service after its export (*i.e.*, for a military or civilian purpose), by itself, is not a factor in determining whether the article or service is subject to the controls of this subchapter.”

16. ITAR jurisdiction extends only to the export of defense articles, defense services, and technical data. For this reason, ITAR does not limit the ability of Defense Distributed or others to distribute CAD files to U.S. persons within the United States for domestic use.

The Commodity Jurisdiction (CJ) process

17. Commodity Jurisdictions, commonly referred to as “CJs,” are the determination made by the Department of State identifying the export control jurisdiction of goods, services and information.
18. The purpose of these determinations is to reach a conclusion as to whether, for purposes of export controls, goods, services, or information are under the jurisdiction of the Department of State pursuant to ITAR or under the jurisdiction of the Department of Commerce, which administers the Export Administration Regulations (EAR).⁵

⁵ A few categories of goods, services, or information are under the jurisdiction of the Department of Energy, Department of Homeland Security, or another Executive Branch agency. Goods, services, or information may also be within the public domain and not subject to export controls at all.

19. Section 120.4 of the ITAR establishes the CJ procedure,⁶ which “is used with the U.S. Government if doubt exists as to whether an article or service is covered by the U.S. Munitions List. It may also be used for consideration of a re-designation of an article or service currently covered by the U.S. Munitions List. The Department must provide notice to Congress at least 30 days before any item is removed from the U.S. Munitions List.” As required by Section 120.4, the determination “entails consultation among the Departments of State, Defense, Commerce, and other U.S. Government agencies and industry in appropriate cases.” In the vast majority of circumstances, the CJ procedure is unnecessary because there is no doubt as to whether an item to be exported is a defense article or defense service.

20. Section 120.4 of the ITAR sets forth the criteria for making a CJ determination: A designation that an article or service meets the criteria of a defense article or defense service, or provides the equivalent performance capabilities of a defense article on the U.S. Munitions List set forth in this subchapter, is made on a case-by-case basis by the Department of State, taking into account:

(i) The form and fit of the article;⁷ and

⁶ See 58 FR 39283, July 22, 1993, as amended at 71 FR 20536, Apr. 21, 2006; 75 FR 46843, Aug. 4, 2010; 78 FR 22753, Apr. 16, 2013; 79 FR 8084, Feb. 11, 2014.

⁷ The form of a commodity is defined by its configuration (including the geometrically measured configuration), material, and material properties that uniquely characterize it. The fit of a commodity is defined by its ability to physically interface or connect with or

(ii) The function and performance capability of the article.⁸

21. Section 120.4(f) further requires that “State, Defense and Commerce will resolve commodity jurisdiction disputes in accordance with established procedures. State shall notify Defense and Commerce of the initiation and conclusion of each case.”
22. Section 120.4(g) provides an avenue for appeal of a CJ determination:

A person may appeal a commodity jurisdiction determination by submitting a written request for reconsideration to the Deputy Assistant Secretary of State for Defense Trade Controls. The Deputy Assistant Secretary's determination of the appeal will be provided, in writing, within 30 days of receipt of the appeal. If desired, an appeal of the Deputy Assistant Secretary's decision can then be made to the Assistant Secretary for Political-Military Affairs.
23. DTCP considers a variety of information in its consideration of CJ requests, including the information attached to the request (such as product brochures, technical specifications and/or blue prints, sales information, etc.), the USML category in which an item most likely may fit, previous CJs on the technology or related matters, and previously-issued export licenses for similar items.

become an integral part of another commodity. [See Note 1 to paragraph (d), section 120.4 of the ITAR.

⁸ The function of a commodity is the action or actions it is designed to perform. Performance capability is the measure of a commodity's effectiveness to perform a designated function in a given environment (e.g., measured in terms of speed, durability, reliability, pressure, accuracy, efficiency).

After DTCP prepares a preliminary analysis, the CJ request and preliminary analysis are circulated to the relevant interagency partners for consultation.

Defense Distributed's CJ Requests

24. In early May, 2013, DTCP became aware through media reports that Defense Distributed (DD), a pending 501(c)(3) non-profit corporation located in Austin, Texas, had placed on an unrestricted website executable Computer Aided Design (CAD) files enabling the manufacture of plastic firearm components, accessories, and attachments with a 3D printer. *See, e.g.*, Exhibit 1.
25. As a result, the Department of State's Office of Defense Trade Controls Compliance (DTCC) became concerned that these files might be subject to the ITAR, in which case DD might be exporting these files without authorization. DTCC therefore sent a letter to DD, suggesting that they remove the files from their website and submit CJ requests to determine whether the files were controlled by the ITAR. *See* Exhibit 2. DD complied with the request and on June 21, 2013, submitted ten CJ requests. *See* Exhibit 3.
26. In its CJ submission, DD identified a number of publicly available sources for information on how to manufacture firearms and related components, including books on gunsmithing and gun design blueprints and schematics available in a variety of media, including on the Internet. DD asserted that their CAD files were no different from any other medium that contains basic manufacturing "know

how” for firearms, and that these files should be found to be in the public domain and not controlled under the ITAR. *See* Exhibit 3.

27. In addition to conferring with other agencies in accordance with ITAR Section 120.4, DTCP sought to better understand additive manufacturing and 3D printing hardware and technology and its evolution and diffusion, the impact of the availability of CAD files (and other, similar data files) on the enforcement of export controls, and the application of multilateral export control regime, particularly the Wassenaar Arrangement on Export Controls on Conventional Arms and Dual-use Goods and Technologies, to such files and technologies. DTCP consulted other State Department offices and U.S. government agencies to benefit from their expertise and consideration of these technologies and issues. In addition, DTCP organized a conference on additive manufacturing/3D printing technology in March 2014.

28. In January 2015, while consideration of DD’s June, 2013 CJ requests was ongoing, DD submitted a CJ request for the “Ghost Gunner,” a computer numerically controlled (CNC) press for milling metal firearms components. *See* Exhibit 4. On April 15, 2015, DDTC responded by providing a CJ determination to Defense Distributed, finding that the Ghost Gunner would not be subject to the jurisdiction of the Department of State. *See* Exhibit 5. In the course of consideration of the Ghost Gunner, DTCP determined that project files and data files for producing a defense article on a 3D printer or similar device constituted technical data on that defense article that would be subject to ITAR jurisdiction.

Resolution of the Ghost Gunner CJ request also helped DTCP conclude the CJ process for DD's June 21, 2013 CJ requests. On June 4, 2015, DTCP provided CJ determinations for the requested items. *See* Exhibit 6.

DDTC's CJ Determination

29. In making its CJ determination, DDTC identified several factors that warrant treatment of DD's CAD files as technical data subject to ITAR jurisdiction.
- a. The central function of DD's executable CAD files appears to be to enable the manufacture of end-items that are ITAR-controlled defense articles.
 - b. As DD described in its Ghost Gunner CJ request, DD's CAD files can be used to "automatically find, align, and mill" a defense article such as a firearm on a 3D printer or other manufacturing device. Manufacture of a defense article in this way requires considerably less know-how than manufacture in reliance on conventional technical data, which merely *guides* the manufacture of a defense article and requires additional craftsmanship, know-how, tools, and materials.
 - c. Although DD contended that the technical data constituted published data already in the public domain, the existing material in the public domain identified by DD did not include CAD files that could be used to automatically generate defense articles. Because CAD files provide the

additional functionality described above, DD's CAD files are a meaningful step beyond previous, public-domain material.

d. In addition, because DD's CAD files are information similar to "blueprints, drawings, photographs, plans, instructions or documentation" that can be used to automatically manufacture defense articles, DDTC concluded that the regulations place them within ITAR commodities jurisdiction.

30. Based on these considerations, its consultations with other State Department offices and U.S. government agencies, its own expertise, and the text of the AECA and ITAR, DDTC concluded that DD's CAD files fall within the jurisdiction of the ITAR as technical data under Category I, subsection (i) of the USML, relying on the definition of technical data in 22 C.F.R. § 120.10(a)(1). DDTC concluded that other information, including a "read-me" file submitted by DD for a CJ determination, did not fall within the jurisdiction of the ITAR. Accordingly, DDTC's determination does not restrict DD from discussing information and ideas about 3D printing, either domestically or internationally, as long as such discussions do not include the export of technical data.

31. Classification of DD's CAD files as within the jurisdiction of the ITAR is not an outright prohibition on the export of these files. Rather, ITAR requires that DD obtain a "license or other approval . . . pursuant to the ITAR prior to any export" for these CAD files.

32. Should DD submit an application for approval to export its CAD files, DDTC will review the proposed export, including its intended recipients and the type, form, and scope of the export. DDTC will consider the application in accordance with the factors enumerated in 22 C.F.R. § 126.7, including whether such export is prohibited “by any statute of the United States.” 22 C.F.R. § 126.7(a), whether such export would be “in furtherance of world peace, the national security or the foreign policy of the United States.” 22 C.F.R. § 126.7(a)(1), whether “[a]n applicant, any party to the export or agreement, any source or manufacturer of the defense article or defense service or any person who has a significant interest in the transaction has been debarred, suspended, or otherwise is ineligible to receive an export license or other authorization from any agency of the U.S. government.” *id.* § 126.7(a)(6). In addition, there are numerous countries to which exports of some or all categories of defense articles are prohibited. *See, e.g.*, 22 C.F.R. § 126.1.

33. In my experience, the overwhelming majority of ITAR licensing applications are approved outright or approved with conditions intended to safeguard the defense article being exported from use in a way that would damage world peace or the national security or foreign policy interests of the United States. Of course, any given licensing application will only be approved if the application satisfies the standards required under 22 C.F.R. § 126.7.

Likely Effects of the Preliminary Injunction Sought by Plaintiffs

34. The entry of a preliminary injunction authorizing the posting of DD's CAD files to the Internet without restriction would make those files available worldwide to any Internet user, thereby permitting the export of those files to any foreign person or foreign power with access to DD's website. Such an injunction would deny DDTC the opportunity to consider, among other things, whether any specific export of DD's CAD files would violate the law or would cause significant harm to the national security or foreign policy interests of the United States.

35. Absent a specific request for an export license, I have considered the likely impacts of an unrestricted export of DD's CAD files to any interested person, entity, or foreign power and concluded that the likely effect of a preliminary injunction would be to cause significant harm to the national security and foreign policy interests of the United States. Although a comprehensive enumeration of the possible harms would be difficult, I can identify the following as among the most concerning:

- a. The "Liberator" firearm included in DD's CAD designs presents a specific and unique risk to the national security and foreign policy interests of the United States. The Liberator is a plastic firearm which can be produced in a way as to be both fully operable and virtually undetectable by conventional security measures such as metal detectors. police and security services, could particularly, (though not uniquely) cause damage U.S. foreign policy interests. If U.S.-origin CAD files were used to

manufacture an undetectable “Liberator” in a foreign country, and that weapons was then used to commit an act of terrorism, piracy, assassination, or other serious crime (e.g., to compromise aviation security overseas), the act itself – or the interests of a foreign country in holding the United States accountable – could cause serious and long-lasting harm to the foreign policy and national security interests of the United States.⁹

- b. The United States and other countries rely on international arms embargoes, export controls, and other measures to restrict the availability of defense articles sought by terrorist organizations. Making DD’s CAD files available through unrestricted access on the Internet would provide any such organization with defense articles, including firearms, at its convenience, subject only to its access to a 3D printer, an item that is widely commercially available. Terrorist groups and other actors could then potentially manufacture and use such weapons against the United States or its allies.
- c. Making DD’s CAD files available through unrestricted access on the Internet would likewise provide access to the firearms components and replacement parts to armed insurgent groups, transnational organized criminal organizations, and states subject to U.S. or UN arms embargoes.

⁹ Undetectable firearms are unlawful in the United States pursuant to the Undetectable Firearms Act of 1988. See 18 U.S.C. § 922(p). Although the “Liberator” design includes insertion of a six-ounce piece of metal to make it detectable by metal detectors, this metal content can be removed without rendering it inoperable, thereby permitting it to be both operable and undetectable.

Access to weapons technology coupled with the uncontrolled and increasingly ubiquitous means of production (i.e., 3D printers or other similar manufacturing technology capable of executing CAD files) could contribute to armed conflict, terrorist or criminal acts, and seriously undermine global export control and non-proliferation regimes designed to prevent the dangerous and destabilizing spread and accumulation of weapons and related technologies. U.S. leadership in these areas also would suffer, contributing overall to a more dangerous international environment.

- d. Many countries, including important U.S. allies, have more restrictive firearms laws than the United States and have identified firearms CAD files for 3D printers as a threat to domestic firearms laws. For example, both the United Kingdom and Japan have arrested individuals for manufacturing or attempting to use firearms CAD files and 3D printers to manufacture firearms. *See, e.g.,* <http://www.bbc.com/news/technology-27322947>, accessed, June 6, 2015. Unrestricted exports from the United States of munitions or technical data, such as DD's CAD files, which could be used to automatically manufacture a firearm or other defense article, would undercut the domestic laws of these nations, increase the risk of domestic violence in those countries, and thereby damage U.S. foreign relations with those countries and foreign policy interests.

36. In my judgment, the entry of a preliminary injunction in this matter would increase the risk of all of the foregoing harms. Indeed, such an injunction could reasonably be expected to bring attention to DD's CAD files, making awareness of their capabilities and accessibility known more widely to individuals, entities, and foreign powers that would make use of DD's CAD files to the detriment of U.S. foreign policy and national security interests.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on June 10, 2015.

A handwritten signature in cursive script, reading "Lisa V. Aguirre", is written above a horizontal line.

Lisa V. Aguirre

EXHIBIT

1

3D-printable guns are just the start, says Cody Wilson

The inventor of 'The Liberator' plastic firearm believes in an open future and the 'complete explosion' of all gun law

Alex Rayner

Monday 6 May 2013 11.56 EDT

Cody Wilson is a polite, 25-year-old law student at the University of Texas in Austin, with dark, close-cropped hair and a forward, affable charm. This week he plans to release the blueprint for a gun that can be downloaded from the internet and produced using a 3D printer.

He and his friends have spent almost a year developing the Liberator, a "Wiki weapon" that can be assembled from components made on an \$8,000 (£5,150) printer that they bought on eBay. Using files shared online, the machine creates the solid parts from layers of plastic.

Wilson's group, Defense Distributed, thinks everyone should have access to a gun and is working to make it possible through Defcad.org, a depository for weapons designs. It was set up in December after its files were removed from another site following the Sandy Hook elementary school shootings. In March, Wilson was issued a federal firearms licence, allowing him to make guns legally.

"I come from a typical middle class family, for the United States in the south: religious parents, conservative values, though we didn't own a lot of firearms," he says. "We had one shotgun that we never really used."

Despite buying a shotgun shortly after turning 21, Wilson says it was his studies, first as an English literature major, then as a law student, that started his interest in the politics of weapons ownership. "I read [19th-century French anarchist theorist Pierre-Joseph] Proudhon," he says, "I like Jean Baudrillard. I like their critiques of mass culture."

He admits that, given current technology, printing a gun is the least effective way of obtaining a firearm, and that it is easier to simply fashion a gun from the contents of any hardware store.

Yet he half hopes, half believes that soon, thanks to the convergence of file-sharing and 3D printing, there will come about "a complete explosion of all available gun laws. I think we should be allowed to own automatic weapons; we should have the right to own all the

terrible implements of war, as [American political philosopher] Henry Coxe said, and I think this principle probably applies globally."

A self-described child of the internet age, Wilson is an admirer of Julian Assange and Kim Dotcom. "I number myself among them, at least in spirit," he says. "I think the future is openness to the point of the eradication of government. The state shouldn't have a monopoly on violence; governments should live in fear of their citizenry."

His ambitions don't stop at firearms. Ultimately, he wants to turn Defcad into "the world's first unblockable open-source search engine for all 3D printable parts", a Pirate Bay-style archive not only for printable pistols, but for everything from prosthetic limbs to drugs and birth-control devices.

More features

Topics

US gun control

Shots fired from world's first 3D-printed handgun

Cody Wilson, 25, successfully tested plastic handgun built by his Texas firm Defense Distributed using an \$8,000 3D printer

Adam Gabbatt in New York

Monday 6 May 2013 14.43 EDT

The world's first gun made almost entirely by a 3D plastic printer has been successfully fired in Texas.

The successful test of the plastic handgun, which was built by Defense Distributed using an \$8,000 3D printer, came after a year of development. The company, which is run by 25-year-old Cody Wilson, now plans to publish the blueprints for the gun online.

Wilson and a companion successfully fired the gun for the first time in Austin, Texas, at the weekend, Forbes reported. A video published online shows the gun held in place by a metal stand, with yellow string attached to its trigger. By yanking on the string, the pair were able to pull the trigger from 20ft away, successfully discharging a .380 caliber bullet.

Defense Distributed's device is controversial because of the way it is made. Fifteen of its 16 pieces were constructed in a second-hand Stratasys Dimension SST 3D printer, Forbes said. The final piece, the firing pin, is a common nail available from any hardware store. The printer used ABS plastic to create the gun parts, which were then slotted together by Wilson. After Forbes's revelation, the BBC filmed a later test, in which Wilson successfully fired the gun by hand.

The Undetectable Firearms Act of 1988 makes it illegal to manufacture in the US any firearm that is not detectable by walk-through metal detectors. To combat this, Wilson inserted a 6oz piece of steel into the body of his gun, making it legal.

How long the law stays this way remains to be seen, however. On Sunday, New York senator Charles Schumer called for legislation to make building a gun with a 3D printer illegal, and said he and the New York congressman Steve Israel would introduce the Undetectable Firearms Modernisation Act, which would ban weapons like Wilson's.

Such an act would not be the first setback for Wilson, a law student at the University of Texas. An attempt to raise money for the 3D printed gun project through Indiegogo was thwarted when the crowdfunding website took his pitch offline, citing a breach of rules. After Wilson raised \$20,000 through Bitcoin donations, he was hindered again when

Stratys seized back his printer.

Defense Distributed acquired a second-hand Stratys, however, and carried on experimenting. Wilson successfully made and tested parts of an AR-15 semi-automatic rifle - the weapon which has been used in a number of mass shootings in the US - before turning his attention to a plastic handgun.

More news

Topics

US gun control

3D printing

3D

EXHIBIT

2



United States Department of State
Bureau of Political-Military Affairs
Office of Defense Trade Controls Compliance
Washington, D.C. 20522-0112

MAY 08 2013

In reply refer to
DTCC Case: 13-0001444

Mr. Cody Wilson
Defense Distributed
711 W. 32nd Street, Apt. 115
Austin, TX 78705

Dear Mr. Wilson:

The Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance, Enforcement Division (DTCC/END) is responsible for compliance with and civil enforcement of the Arms Export Control Act (22 U.S.C. 2778) (AECA) and the AECA's implementing regulations, the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130) (ITAR). The AECA and the ITAR impose certain requirements and restrictions on the transfer of, and access to, controlled defense articles and related technical data designated by the United States Munitions List (USML) (22 C.F.R. Part 121).

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEFCAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

Technical data regulated under the ITAR refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, including information in the form of blueprints, drawings, photographs, plans, instructions or documentation. For a complete definition of technical data, see § 120.10 of the ITAR. Pursuant to § 127.1 of the ITAR,

it is unlawful to export any defense article or technical data for which a license or written approval is required without first obtaining the required authorization from the DDTC. Please note that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is considered an export under § 120.17 of the ITAR.

The Department believes Defense Distributed may not have established the proper jurisdiction of the subject technical data. To resolve this matter officially, we request that Defense Distributed submit Commodity Jurisdiction (CJ) determination requests for the following selection of data files available on DEFCAD.org, and any other technical data for which Defense Distributed is unable to determine proper jurisdiction:

1. Defense Distributed Liberator pistol
2. .22 electric
3. 125mm BK-14M high-explosive anti-tank warhead
4. 5.56/.223 muzzle brake
5. Springfield XD-40 tactical slide assembly
6. Sound Moderator – slip on
7. “The Dirty Diane” 1/2-28 to 3/4-16 STP S3600 oil filter silencer adapter
8. 12 gauge to .22 CB sub-caliber insert
9. Voltlock electronic black powder system
10. VZ-58 front sight.

DTCC/END requests that Defense Distributed submit its CJ requests within three weeks of receipt of this letter and notify this office of the final CJ determinations. All CJ requests must be submitted electronically through an online application using the DS-4076 Commodity Jurisdiction Request Form. The form, guidance for submitting CJ requests, and other relevant information such as a copy of the ITAR can be found on DDTC’s website at <http://www.pmddtc.state.gov>.

Until the Department provides Defense Distributed with final CJ determinations, Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately. Defense Distributed should also review the remainder of the data made public on its website to

- 3 -

determine whether any additional data may be similarly controlled and proceed according to ITAR requirements.

Additionally, DTCC/END requests information about the procedures Defense Distributed follows to determine the classification of its technical data, to include the aforementioned technical data files. We ask that you provide your procedures for determining proper jurisdiction of technical data within 30 days of the date of this letter to Ms. Bridget Van Buren, Compliance Specialist, Enforcement Division, at the address below:

Office of Defense Trade Controls Compliance
PM/DTCC, SA-1, Room L132
2401 E Street, NW
Washington, DC 20522
Phone: 202-663-3323.

We appreciate your full cooperation in this matter. Please note our reference number in any future correspondence.

Sincerely,



Glenn E. Smith
Chief, Enforcement Division

EXHIBIT

3

WILLIAMS MULLEN

Jahna M. Hartwig
Direct Dial: 202.293-8145
jhartwig@williamsmullen.com

June 21, 2013

Ms. Sarah Heidema
U.S. Department of State
Directorate of Defense Trade Controls
PM/DDTC, SA-1, Room 1200
2401 E Street, NW
Washington, DC 20037

Subject: Commodity Jurisdiction Requests for Data Files Posted by Defense Distributed

Enclosures: (1) Printouts of Drawings from Files Posted at DEFCAD.org
(2) Wikipedia Page for 125mm BK-14M HEAT
(3) Thingiverse Page for Sound Moderator
(4) Thingiverse Page for VZ-58 Front Sight
(5) Examples of Solvent Trap Adapters
(6) Examples of CAD Files for .22 Pistols
(7) Examples of CAD Files for Muzzle Brakes
(8) Examples of CAD Files for Slide Assemblies
(9) Examples of CAD Files for Voltlock System

Dear Ms. Heidema:

Defense Distributed has been requested by DTCC/END to submit requests for commodity jurisdiction determinations in connection with Case No. 13-0001444 for ten sets of data files posted to DEFCAD.org. As demonstrated below, the files are primarily Computer Aided Design (CAD) data files and should be considered public domain information that is excluded from the ITAR pursuant to Section 120.11. Defense Distributed therefore respectfully requests a determination that these files are not subject to the ITAR.

COMMODITY DESCRIPTIONS

Each of these Commodity Jurisdiction requests relates to data files, almost all of which are essentially blueprints that can be read by CAD software. A description of each file or set of files is set out below. The files are in one of the following formats:

- STL (STereoLithography or Standard Tessellation Language) is a file format native to the stereolithography CAD software and can be used with some 3D printers. "Stereolithography" is a means of creating physical 3D models of objects using resin or carefully cut and joined pieces of paper. STL files describe only

the surface geometry of a three dimensional object without any representation of color, texture or other common CAD model attributes.

- The IGS (Initial Graphics Exchange Specification) file format is the standard format for transferring three-dimensional models between CAD programs. IGS files can store wireframe models, surface or solid object representations, circuit diagrams, and other objects.
- SLDPRT is the proprietary image file format associated with the SolidWorks brand CAD software. SLDPRT files contain three-dimensional images of one specific part of a product.
- SKP is the CAD drawing format for Google Sketchup, which is a quick, entry-level 3D drawing program.

There are also a small number of Word (.DOC), text (.TXT) or image (.JPG or .BMP) files. A printout of each file is attached to the relevant DS-4076.

As explained further below, each of these files either was previously placed in the public domain or contains only public domain information.

1. Liberator Pistol Data Files

The files for the Liberator Pistol include sixteen STL files for the various parts and components of the pistol, two "read me" text files that explain how to lawfully assemble the pistol, a diagram of a pistol, and a permissive software license. If printed on a 3D printer, the parts could be assembled into a single shot .380 caliber firearm.

2. .22 Electric Data Files

The files for the .22 Electric are two stereolithography (STL) CAD files for models of a barrel and grip for a .22 caliber pistol. If printed, the barrel would be a plastic cylinder with a .22 mm bore and the grip would be a plastic piece with two 5mm diameter holes. If those pieces were printed in plastic and used with an electronic system and firing mechanism, the barrel would be expected to fail upon firing.

3. 125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File

The file is a STL CAD file for a model of a BK-14M high explosive anti-tank warhead without fins. The model, if printed on a 3D printer, would be a solid piece of plastic in the shape of the warhead, but would not be capable of functioning as a warhead.

4. 5.56/.223 Muzzle Brake Data Files

The data files are three different CAD file formats (.IGS, .SLDPRT, and .STL) for a model of a 5.56/.223 muzzle brake. If printed on a 3D printer, the model would be a plastic piece in the shape of the muzzle brake, but would be expected to fail if used with a weapon.

5. Springfield XD-40 Tactical Slide Assembly Data Files

The files are nineteen Computer Aided Design (CAD) data files in the SolidWorks .SLDPRT file format for models of components of a pistol slide for the Springfield XD-40. The

Defense Distributed CJ Requests
 June 21, 2013
 Page 3

components, if printed on a 3D printer, would be plastic pieces in the shape of the components of the slide assembly, but would be expected to fail if used with a weapon.

6. Sound Moderator – Slip On File

The file is a stereolithography CAD file for a model of a slip-on sound moderator for an air gun. The model, if printed on a 3D printer, would work with an air gun, but would likely melt if used with a firearm.

7. “The Dirty Diane” ½-28 to ¾-16 STP S3600 Oil Filter Silencer Adapter Files

The file is a CAD data file in the SolidWorks .SLDPRT file format for a model of an oil filter silencer adapter that is typically produced in stainless steel. If printed on a 3D printer, this item could be used as a solvent trap adapter, which is used to catch solvents that are used in the process of cleaning a gun. While a metal solvent trap adapter could be used as a silencer, a plastic adapter would likely melt if used with a weapon as a silencer.

8. 12 Gauge to .22 CB Sub-Caliber Insert Files

The files are a SKP CAD file for a model of a sub-caliber insert, two renderings of the sub-caliber insert, and a “read me” text file providing information about the National Firearms Act and the Undetectable Firearms Act. This item, if printed on a 3D printer, would be a plastic cylinder with a .22 bore, and would be expected to fail if used with a weapon.

9. Voltlock Electronic Black Powder System Files

The files are twelve CAD files for models of cylinders of various bores with a touch hole. Eleven of the files are in the STL file format and one is in the IGS format. If those pieces were printed on a 3D printer and used with an electronic ignition, the barrel would be expected to fail.

10. VZ-58 Front Sight Files

The files are a SolidWorks CAD file in the .SLDPRT file format and a rendering of a model of a sight for a VZ-58 rifle. If printed on a 3D printer and used with a weapon, the sight would be expected to fail.

DATA ORIGIN

With the exception of item 1 (Liberator Pistol Data Files), each of these files was provided to Defense Distributed by the creator of the files identified in the DS4076. In addition, as explained below, many of these files were originally posted to www.thingiverse.com or other internet sites, and were freely available to any person with access to the internet.

The Liberator Pistol CAD files were developed by Defense Distributed. The Liberator pistol was designed as a combination of already extant and working files and concepts. The pistol frame, trigger housing, and grip specifications were all taken directly from an AR-15 lower receiver file that is in the public domain. The spring file is taken from a toy car file available on Thingiverse. The hammer relies on striking a common roofing nail, and the barrel is a cylinder bored for .380. The gun functions because of the properties of the .380 cartridge – the brass

Defense Distributed CJ Requests

June 21, 2013

Page 4

casing itself is relied on to act as a breech. The printed and assembled gun is a simple improvised weapon, not as complex as many of the improvised weapons of the 20th century, those available in Army manuals, etc. All of the technologies used to create the Liberator data files are widely available in the public domain.

IDENTICAL & SIMILAR FILES

The Liberator Pistol data files are for an improvised firearm that is similar to and based on numerous items that are available on the internet as well as in various books. The Library of Congress online catalog lists numerous books on gunsmithing, including

- Clyde Baker, Modern gunsmithing; a manual of firearms design, construction, and remodeling for amateurs & professionals (1959)
- John E. Traister, Clyde Baker's Modern gunsmithing : a revision of the classic (1981)
- Frank de Haas, Mr. Single Shot's gunsmithing idea book (1983)
- Roy F. Dunlop, Gunsmithing (1996),
- Franklin Fry, Gunsmithing fundamentals : a guide for professional results (1988),
- James Virgil Howe, The modern gunsmith : a guide for the amateur and professional gunsmith in the design and construction of firearms, with practical suggestions for all who like guns (1982),
- Gérard Métral, A do-it-yourself submachine gun: it's homemade, 9mm, lightweight, durable, and it'll never be on any import ban lists! (1995),
- Jack Mitchell, The Gun digest book of pistolsmithing (1980),
- J. Parrish Stelle, The gunsmith's manual; a complete handbook for the American gunsmith (1883), and
- Patrick Sweeney, Gunsmithing: pistols & revolvers (2009),

among many others. Examples of online sources include:

- <http://www.weaponscombat.com/zip-pipe-and-pen-guns>
- <http://www.infinitearms.com/images2/v/manuals/Misc+Gun+Plans>
- <http://thehomegunsmith.com>
- <http://www.scribd.com/doc/24445441/Pen-Gun-Mk1-Blueprint>
- https://www.google.com/search?q=zip+gun+blueprints&rlz=1C1SKPM_enUS436US489&source=lnms&tbn=isch&sa=X&ei=9t-oUZybJILm8wSx0YHoBg&ved=0CAoQ_AUoAQ&biw=1600&bih=837
- <http://ebookbrowse.com/gu/guns-homemade>

Although DD converted this information into CAD file format, DD does not believe that it created any new technical data for the production of the gun.

A drawing of the 125 BK-14M HEAT (Item 3), including measurements, is currently available on Wikipedia at http://en.wikipedia.org/wiki/File:125mm_BK-14m_HEAT.JPG.

Defense Distributed CJ Requests
June 21, 2013
Page 5

The Sound Moderator CAD file (Item 6) was published on Thingiverse on March 3, 2011 and is still available on that site at <http://www.thingiverse.com/thing:6808>. The VZ-58 Front Sight (Item 10) was also published to Grabcad on December 14, 2012 and is still available on that site at <http://grabcad.com/library/front-sight-for-vz-dot-58-rifle>.

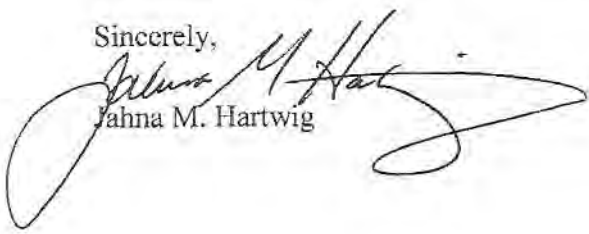
The Oil Filter Silencer Adapter is identical to Solvent Trap Adapters, which are produced by numerous manufacturers and available as commercial products on many websites, including amazon.com. (see http://www.amazon.com/s/ref=nb_sb_noss_1?url=search-alias%3Dautomotive&field-keywords=solvent+trap+adapter&rh=n%3A15684181%2Ck%3Asolvent+trap+adapter.) These items appear to be commercial products that would be subject to the EAR. As such, any related technologies or technical data would also be subject to the EAR.

Examples of CAD files similar to the .22 Electric Pistol (Item 2), Muzzle Brake (Item 4), Slide Assembly (Item 5), and Voltlock Electronic Black Powder System (Item 9) that are currently available on the internet are attached to the relevant DS4076.

As demonstrated above, all of the technical information included in the data files posted to DEFCAD.org was previously available in the public domain. As such, this information is excluded from the definition of "technical data" by 22 C.F.R. § 120.10(a)(5). For these reasons, Defense Distributed respectfully requests that the Department determine that the subject data files posted to DEFCAD.org are not subject to the ITAR.

This submission contains Defense Distributed confidential business information. We respectfully request that the submission be kept confidential. If you need additional information regarding this submission, please contact me at 202-293-8145 or jhartwig@williamsmullen.com.

Sincerely,


Jahna M. Hartwig

EXHIBIT

4

MATTHEW A. GOLDSTEIN, PLLC

1012 14TH STREET, NW, SUITE 820
WASHINGTON, DC 20005

VIA ELECTRONIC FILING

January 2, 2015

PM/DDTC, SA-1, 12th Floor
Office of Defense Trade Controls
Bureau of Political Military Affairs
U.S. Department of State
Washington, D.C. 20522-0012

SUBJECT: Commodity Jurisdiction Request for Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software (Defense Distributed, Inc., PM/DDTC Code M-34702)

Dear Sir or Madam:

Pursuant to Section 120.4 of the International Traffic in Arms Regulations ("ITAR") (22 C.F.R. Sections 120-130), Defense Distributed requests a commodity jurisdiction determination from the Directorate of Defense Trade Controls ("DDTC") on the Ghost Gunner machine (the "Ghost Gunner"), its plastic mounting jig, user instructions, and software for production, operation, and use of the Ghost Gunner.

The Ghost Gunner is an approximately one-foot-cubed black box that uses a drill bit mounted on a head that moves in three dimensions to automatically carve digitally-modeled shapes into polymer, wood or aluminum. It functions as a 3-axis computer-numerically-controlled ("CNC") press that can be used to manufacture parts to firearms controlled under U.S. Munitions List ("USML") Category I. It can also be used to manufacture items that are not controlled under the USML. The machine was designed, developed, and manufactured by Defense Distributed to automatically manufacture publicly available designs with nearly zero user interaction.

As discussed below, the Department of Defense recommended that Defense Distributed submit this commodity jurisdiction request.

Export jurisdiction over the Ghost Gunner, Jig, software, and instructions is uncertain because, although the Department of Commerce Export Administration Regulations ("EAR") maintain a control listing for jigs, fixtures, and other metal-working items "exclusively designed for use in the manufacture of firearms" under Commerce Control List ("CCL") Export Control Number ("ECCN") 2B018.n, there is no corresponding carve-out for these items and related software and technical information otherwise controlled by USML Category I generally; and Category I(i) controls technical data and defense services directly related to firearms, with technical data directly related to the manufacture or production of firearms designated as Significant Military Equipment.

Please note that a letter from Defense Distributed authorizing my law firm to file this request was uploaded with this DS-4076 submission. Please direct any questions and all correspondence related to this request to my office. Communications to me at matthew@goldsteinpllc.com are preferred.

I. BACKGROUND

A. Defense Distributed

Defense Distributed is a Texas corporation, registered with the Department of State under PM/DDTC Code M-34702. The company has developed technical information that can be used to produce, manufacture, and assemble various parts components, accessories, and attachments to firearms controlled under USML Category I. This includes information for the design and production of the Ghost Gunner, software necessary to operate Ghost Gunner, and code that allows production of certain items by the Ghost Gunner.¹

Following notification from DDTC in May 8, 2013, that the agency requires U.S. Government prior approval before publications of otherwise ITAR-controlled technical data into the public domain (Attachment 1), Defense Distributed has submitted requests for U.S. Government clearance of technical data to the Department of Defense Office of Prepublication and Security Review ("DOPSR").² On October 1, 2014, DOPSR returned a Defense Distributed request for clearance of technical information on the Ghost Gunner for public release, stating that commodity jurisdiction over the item was uncertain and recommending that Defense Distributed submit a commodity jurisdiction request. See Attachment 2.

B. The Ghost Gunner

Existing CNC machines are expensive or too inaccurate to manufacture firearms for the casual user. Defense Distributed developed the Ghost Gunner to address this problem by miniaturizing the build envelope to just large enough to mill common firearm receivers, which in turn improves rigidity, reduces material cost and simultaneously relaxes certain design limits, allowing Defense Distributed to sell an inexpensive machine with more than enough accuracy to manufacture firearms.

The first design tested on the Ghost Gunner was for an AR-15 lower receiver and the Ghost Gunner was able to automatically find, align, and mill a so-called "80%" lower receiver, which was not a firearm prior to milling. The Ghost Gunner has since undergone several design revisions to reduce machine chatter, backlash, and jitter, all with the goal of keeping total design cost low.

Photographs of Ghost Gunner are provided at Attachment 3 and rendered images of the machine with the plastic jig are provided at Attachment 4.

¹ This commodity jurisdiction request seeks a determination of the code necessary to operate Ghost Gunner. It does not seek a determination on the various project files specific to production of certain items by the Ghost Gunner.

² In complying with DDTC prepublication review requirements on publication of technical information into the public domain, Defense Distributed does not intend to, nor should it be considered to, waive any defense, claim or right under law.

A schematic drawing for the Ghost Gunner is provided at Attachment 5.

Ghost Gunner form, fit, function, and performance characteristics include the following:

- It uses a compact, powder coated A36 steel frame and thick stainless T-slot rail, with preloaded ball bearings for maximum rigidity. Linear motion is achieved with low-backlash direct-drive ball screws mounted in-line with the cutting surface, thus preventing torsional gantry chatter while machining.
- It incorporates an electronic probe that automatically detects when the machine comes into contact with the work piece, allowing automatic part discovery and alignment. Ghost Gunner requires conductive parts if auto-discovery and alignment are used.
- It can manually machine nonconductive materials, but this requires manual calibration of a part to the machine - following a few simple instructions - as is required with existing CNC machines.
- Its moving parts are entirely sealed from chip debris. All bearings are sealed and contain wipers to prevent foreign contaminate entry. The rails are stainless steel and are factory lubricated, but do require periodic wiping to prolong life. End Mills dull over time and are considered a consumable.
- To contain aluminum chips, it includes a chip collection tray and all moving components are fully enclosed.
- It is capable of manufacturing deep pockets due to its horizontal gantry, which allows gravity to pull chips away from the cutting surface before they can build up and dull the end mill, as is the case on traditional CNC designs.
- It uses industry standard ER-11 collets, and ships with both 1/4" and 5/32" collets.
- It uses a standard IEC power cord and is compatible with any 110/220V circuit. No external power brick is used; the machine is entirely self-contained.
- It has two ports: Power (IEC standard) and USB (Type 'B').
- Its machinable dimensions are 140 x 75 x 60mm (~5.50 x 2.95 x 2.35")
- Its maximum part dimensions are 230 x 90 x 100mm (~9.05 x 3.50 x 3.90")
- Its overall footprint is 330 x 280mm (~13 x 11")
- Its weight is 20kg (~45 pounds)

- Its Spindle Speed is 10,000+ RPM (Final Value TBD)
- Its software requirements are Windows 7 or higher. Mac version TBD

As noted above, Ghost Gunner is capable of manufacturing more than just firearm receivers. With Defense Distributed's open source Physibles Development SDK ("pDev"), designers can distribute files via the company's '.dd' file format, which contains all installation and assembly instructions, any required jig files to hold a part in place (that users can print with a 3D printer), and all machine definitions and code to physically manufacture a particular design. To a casual user, the .dd file is a one-stop solution to manufacturing any aluminum physible that the public can design to fit into the build envelope. Defense Distributed will be developing in and supporting this format.

The .dd file format is itself open source and not constrained to the Ghost Gunner or Defense Distributed; any user can define any existing machine's specific parameters via the machine parameters list. A single file can contain specific code and installation instructions for any number of machines. A user with both a Ghost Gunner and a Tormach P1100 could manufacture a particular .dd file on either machine and manufacture the same physible with zero additional user knowledge, as only the instructions required for a particular machine are revealed to the end user. The .dd file format is a CNC response to 3D printing's universal .stl file format. However, Ghost Gunner will also accept TinyG code from any CAM program.

In operation, users provide the parts for milling. They can then simply plug their computer into the Ghost Gunner, install the Ghost Gunner software, and download any compatible .dd design file. 3D printable jigs are used to hold each part in place as each milling step is performed. For example, milling an eighty percent AR-15 lower receiver requires two jig pieces to secure the lower in place while the trigger pocket is milled, and then two more jig pieces are installed to drill the trigger pinholes. As most eighty percent firearms require deep pocket milling, Ghost Gunner's mounting table is parallel to the end mill shaft. This orientation maximizes 3D printed jig strength, minimizes jig complexity, and mechanically aligns the part to the machine upon insertion into the Maker Slide-patterned, Open Source T Slot stainless rails.

Defense Distributed expects its typical order fulfillment will contain the fully assembled Ghost Gunner CNC, plastic mounting jig designed to secure 80% AR-15 receivers, operating software and instructions. Defense Distributed also intends to place instructions and computer code needed to build and use Ghost Gunner into the public domain as Open Source technology.

Block 13 ("Sales information") is not provided with this request because the Ghost Gunner is still in development as Defense Distributed awaits arrival of various production pieces and continues to make any required changes to the product. As such, the company has not yet delivered any machines (i.e., no completed sales). However, the company has accepted 469 pre-orders and 413 advance deposits from prospective purchasers. Each of these orders, except for one, are intended for domestic sale. In addition, consistent with U.S. law, final sales will carry conditions that limit purchases to private use (i.e., not for commercial or military use).

C. User Instructions and Operating Software for the Ghost Gunner

The current draft User Instructions for the Ghost Gunner accompanies this commodity jurisdiction request at Attachment 6. It contains information on how to attach a “80%” lower receiver to Ghost Gunner, such that Ghost Gunner can mill and drill all required holes to transform the lower receiver into a firearm. Ghost Gunner presents numerous User Instructions, User Graphics, and User Selections to the operator. Ghost Gunner performs work via Calibration Code and Milling Code. Ghost Gunner also assists the user in creating 3D printable Jigs, if needed.

The software necessary to produce and operate the Ghost Gunner includes AutoDesk Inventor and a simple executable application that can interpret CNC part files and TinyG code. Additional information detailing the purpose, function, and capability of the software, as requested by DDTC’s DS-4076 Commodity Jurisdiction (CJ) Guidance for Software, accompanies this commodity jurisdiction request at Attachment 7.

II. COMMODITY JURISDICTION STANDARD

The standard applicable to Department of State and other agency considerations of commodity jurisdiction is set forth at ITAR Section 120.3. ITAR Subsection 120.3(a) extends Department of State jurisdiction to any item that meets the criteria of a defense article described on the USML or that provides equivalent performance capabilities; and ITAR Section 120.3(b) provides that a specific article not presently described on the USML shall be determined in the future as a defense article if it provides a critical military or intelligence advantage.

A. Relevant USML Control Listings

Subparagraph (h) to USML Category I controls components, parts, accessories, and attachments for firearms to .50 caliber inclusive. The Ghost Gunner does not meet the Category I(h) criteria because it is not a component or part to a firearm. Rather, it is a machine that can be used for the manufacture of such articles.

Subparagraph (i) to USML Category I controls technical data, to include “software” as defined at Section 120.45(f), and defense services directly related to the firearms and components, parts, accessories, and attachments for firearms to .50 caliber inclusive. Technical data directly related to the manufacture or production of firearms controlled in Category I is designated as Significant Military Equipment.

The USML does not contain a control listing that describes items used for the manufacture of firearms. Instead, that listing is contained on the EAR Commerce Control List (“CCL”) entry for ECCN 2B018.n, which controls “Jigs and fixtures and other metal-working implements or “accessories” of the kinds exclusively designed for use in the manufacture of firearms. ECCN 2D018 controls software” for the “development”, “production” or “use” of equipment controlled by 2B018; and ECCN 2E018, in turn, controls “Technology” for the “use” of equipment controlled by 2B018.

The scope of the CCL controls on firearms manufacturing equipment and technology is unclear because the EAR only controls items not described on the USML and Category I does not contain any carve-out from ITAR control for software or technology controlled under ECCNs 2D018 and 2E018. To the contrary, if literally applied, USML Category I(i) treats such technical information as Significant Military Equipment.

Because there is no specific carve-out in Category I or elsewhere in the USML for software or technology controlled by 2D018 and 2E018, it is very difficult to distinguish between technical data for the manufacture or production of firearms controlled in Category I and technology for the development, production, and use of equipment used to manufacture firearms controlled at 2D018 and 2E018. This is a primary concern of the present commodity jurisdiction request.

Nevertheless, EAR control is consistent with U.S. Implementation of Wassenaar Controls. Specifically, ECCNs 2B018, ECCN 2E018, and 2B018 are Wassenaar Arrangement-based controls, subject to the National Security reason for control and which correspond to Category 2 of the Wassenaar Arrangement List of Dual-Use Items. In fact, 2B018 is titled, "Equipment on the Wassenaar Arrangement Munitions List."

Although relevant text of the ITAR and EAR control listings lack clarity, it appears that the U.S. Government decided to implement export controls on firearms manufacturing equipment and associated technical information in the EAR when it first implemented the Wassenaar Arrangement controls for such items. Accordingly, Defense Distributed believes that the Ghost Gunner does not meet criteria of a defense article described on the USML and that it does not provide equivalent performance capabilities to an article described on the USML.

Defense Distributed further notes that the DDTC should consider amending USML Category I to provide an express carve-out for EAR items controlled under ECCNs 2B018.n, ECCN 2E018, and 2B018. Alternatively, if DDTC intends to control firearms manufacturing equipment under the USML, it should make this clear in the regulations. Towards this end, any determination on the instant request that imposes ITAR control should be widely disseminated and shared with the firearms manufacturing industry.

B. Ghost Gunner Does Not Provide a Critical Military or Intelligence Advantage.

As noted above, ITAR Section 120.3(b) provides that a specific article not presently described on the USML shall be determined in the future as a defense article if it provides a critical military or intelligence advantage.

The function and performance of the Ghost Gunner does not provide a critical military or intelligence advantage. Rather, it is essentially a jig press based on a simple design that is easily replicated by any skilled machinist. In fact, the Ghost Gunner can be produced by persons with no formal engineering background.

In addition, Ghost Gunner builds on technology readily available in the Open Source community, including the gshield 3 axis motion hardware (<http://synthetos.myshopify.com/products/gshield-v5>), the grbl g-code parser and motion controller (<https://github.com/grbl/grbl>), and the Arduino microcontroller (<http://arduino.cc>).

Further, instructions and/or electronic files for production of jig presses with similar form, fit, and function to the Ghost Gunner are publicly available for download at a variety of web addresses, to include the following:

<http://aresarmor.com/store/Item/Polymer-80-Black>
<http://www.thingiverse.com/thing:160266>
https://github.com/DefiantCad/defcad-repo/tree/master/Rifles/AR-15_80_percent_lower_v5-shadowfall/AR-15_80_percent_Lower_Drill_Jig_v1-Shadowfall
<http://www.advancedrifles.com/3d-printed-jig-version-2-0/>
<http://www.80percentarms.com/products/80-ar-15-easy-jig>
<http://www.sierranevadaarms.com/jig.pdf>
<http://www.rockethub.com/projects/24384-80-lower-receiver-ar15-ar10-rudius-1911>

III. CONCLUSION

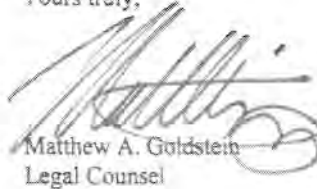
Considering the apparent intent of the U.S. Government in implementing relevant Wassenaar Arrangement controls in the EAR, Defense Distributed believes that the Ghost Gunner does not meet the criteria of an article described on the USML. In addition, the Ghost Gunner does not provide a critical military or intelligence advantage. Accordingly, Defense Distributed respectfully requests that the Department of State issue a commodity jurisdiction determination stating that the Ghost Gunner, its plastic mounting jig, operating software, and production and operation instructions do not meet the criteria of ITAR 120.3 and are subject to Department of Commerce jurisdiction under the EAR.

Defense Distributed authorizes the release for general publication of the information contained in Block 5 of the DS-4076 Form. However, other information in this request and documents submitted with Defense Distributed's DS-4076 Submission contain sensitive business information that is proprietary, confidential, and exempt from disclosure under the Freedom of Information Act, 5 U.S.C. Section 552, and is also protected under the Trade Secrets Act, 18 U.S.C. Section 1905. Accordingly, pursuant to ITAR Section 130.15, Defense Distributed requests that information in this submission other than that contained in Block 5 be withheld in the event of a request for its disclosure.

Commodity Jurisdiction Request
January 2, 2015
Page 8 of 9

Thank you for your prompt attention to this matter and please contact me at 202-550-0040 or at matthew@goldsteinpllc.com if any additional information is needed.

Yours truly,


Matthew A. Goldstein
Legal Counsel

COMPANY CERTIFICATION:

Cody Wilson, the Principal of Defense Distributed, certifies that he is the duly authorized representative of Defense Distributed; and that in such capacity, he certifies that he has carefully read the foregoing Commodity Jurisdiction request; and that the contents of the request are true and correct to the best of his knowledge, information and belief after reasonable inquiry into the matters discussed.


Signature

1/2/2015
Date

ATTACHMENTS TO LETTER OF EXPLANATION:

- | | |
|--------------|--|
| Attachment 1 | May 8, 2013 DDTC Letter to Defense Distributed |
| Attachment 2 | October 1, 2014 DOPSR Letter to Defense Distributed |
| Attachment 3 | Photographs of Ghost Gunner Machine |
| Attachment 4 | Rendered Images of Ghost Gunner Machine |
| Attachment 5 | Ghost Gunner Schematics |
| Attachment 6 | Ghost Gunner User Instructions |
| Attachment 7 | Answers to DS-4076 Commodity Jurisdiction (CJ) Guidance for Software |

www.GoldsteinPLLC.com

Commodity Jurisdiction Request
January 2, 2015
Page 9 of 9

OTHER ATTACHMENTS INCLUDED WITH DS-4076 SUBMISSION:

DD_DS4076.pdf

DD_Attorney_Authorization_Letter_Block_2-1.pdf

[Instant document] DD_Cover_Ltr_Block_6-1.pdf

DD_Certification_Block_19-1.pdf

EXHIBIT

5



United States Department of State

Bureau of Political-Military Affairs
Directorate of Defense Trade Controls

Washington, D.C. 20522-0112

In Reply refer to
DDTC Case CJ 1083-14 (RE-ISSUE)

APR 15 2015

YOUR SUBMISSION DATED: January 2, 2015

COMMODITY JURISDICTION DETERMINATION FOR: **Ghost Gunner Machine, Plastic Mounting Jig, User Instructions, and Software**

The product described in your submission is a one cubic foot box that functions as a 3-axis, computer-numerically-controlled (CNC) press capable of automatically milling parts out of various materials through software designs.

A technical review of your commodity jurisdiction (CJ) request has been concluded by the requisite agencies of the United States Government. A split jurisdiction determination of this request has been determined, as follows:

The Department of State has determined that the **Ghost Gunner, its plastic mounting jig, operating software, and production and operation instructions are not subject to the jurisdiction of the Department of State.** However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **project files, data files, or any form of technical data for producing a defense article, including an 80% AR-15 lower receiver, are subject to the jurisdiction of the Department of State in accordance with the International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130).** They are

Continued on Page Two

Cody R. Wilson
Defense Distributed, Inc.
1101 W 34th Street, #340
Austin, TX 78705
crw@defdist.org

Page Two

In Reply refer to
DDTC Case CJ 1083-14

designated as technical data under Category I(i) of the United States Munitions List (USML). A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not agree with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not agree with this determination and have no additional facts to present, you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Samuel Harmon at (202) 663-2811 or HarmonSC@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com

EXHIBIT

6



United States Department of State

*Bureau of Political-Military Affairs
Directorate of Defense Trade Controls*

Washington, D.C. 20522-0112

In Reply refer to
DDTC Cases CJ 651-13 through 660-13

JUN 04 2015

YOUR SUBMISSION DATED: June 21, 2013

COMMODITY JURISDICTION DETERMINATIONS FOR: Liberator Pistol Data Files, .22 Electric Data Files, 125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File, 5.56/.223 Muzzle Brake Data Files, Springfield XD-40 Tactical Slide Assembly Data Files, Sound Moderator - Slip On Data File, "The Dirty Diane" Oil Filter Silencer Adapter Data File, 12 Gauge to .22 CB Sub-Caliber Insert Data Files, Voltlock Electronic Black Powder System Data Files, and VZ-58 Front Sight Data Files

The data described in your submission are Computer Aided Design (CAD) data files that can be used in a 3D printer to produce physical models of the associated item.

A technical review of your commodity jurisdiction (CJ) request has been concluded by requisite agencies of the United States Government. The findings of that technical review are:

The Department of State has determined that the **125 mm BK-14M High Explosive Anti-Tank Warhead Model Data File, Sound Moderator - Slip On Data File, and "The Dirty Diane" Oil Filter Silencer Adapter Data File** are not subject to the jurisdiction of the Department of State. The Department of Commerce (DOC) advises that these items are classified as EAR99. Please consult the DOC Office of Exporter Services at (202) 482-4811 to satisfy applicable requirements prior to export.

The Department of State has determined that the **Voltlock Electronic Black Powder System Data Files** are not subject to the jurisdiction of the

Continued on Page Two

Cody R. Wilson
Defense Distributed
711 W. 32nd Street, Apt. 115
Austin, TX 78705
crw@defdist.org

Page Two

In Reply refer to
DDTC Cases CJ 651-13 through 660-13

Department of State. However, export may require authorization from the Department of Commerce (DOC). Please consult the DOC Office of Exporter Services at (202) 482-4811 to make a Classification Request (CCATS) and satisfy other applicable requirements prior to export.

The Department of State has determined that the **Liberator Pistol Data Files, .22 Electric Data Files, 5.56/.223 Muzzle Brake Data Files, Springfield XD-40 Tactical Slide Assembly Data Files, 12 Gauge to .22 CB Sub-Caliber Insert Data Files (except for "read me" text file), and VZ-58 Front Sight Data Files** are subject to the jurisdiction of the Department of State in accordance with the **International Traffic in Arms Regulations (ITAR) (22 CFR 120 through 130)**. They are designated as technical data under Category I(i) of the United States Munitions List (USML) pursuant to §120.10 of the ITAR. A license or other approval is required pursuant to the ITAR prior to any export or temporary import.

Should you not concur with this determination and have additional facts not included in the original submission, you may submit a new CJ request. If you do not concur with this determination and have no additional facts to present, then you may request that this determination be reviewed by the Deputy Assistant Secretary of State for Defense Trade Controls.

Should you require further assistance on this matter, please contact Sam Harmon at (202) 663-2811 or HarmonSC@state.gov.

Sincerely,



C. Edward Peartree

Director

Office of Defense Trade Controls Policy

Cc: Matthew A. Goldstein
1012 14th Street, NW, Suite 620
Washington, DC 20005
matthew@goldsteinpllc.com

EXHIBIT

7

hearing," which are conducted pursuant to the provisions of 5 U.S.C. 556 and 557. The CSA sets forth the criteria for scheduling a drug or other substance and for removing a drug or substance from the schedules of controlled substances. Such actions are exempt from review by the Office of Management and Budget (OMB) pursuant to section 3(d)(1) of Executive Order 12866 and the principles reaffirmed in Executive Order 13563.

Executive Order 12988

This regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 Civil Justice Reform to eliminate drafting errors and ambiguity, minimize litigation, provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

Executive Order 13132

This rulemaking does not have federalism implications warranting the application of Executive Order 13132. The rule does not have substantial direct effects on the States, on the relationship between the Federal Government and the States, or the distribution of power and responsibilities among the various levels of government.

Executive Order 13175

This rule does not have tribal implications warranting the application of Executive Order 13175. This rule does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

Regulatory Flexibility Act

The Administrator, in accordance with the Regulatory Flexibility Act (5 U.S.C. 601–612) (RFA), has reviewed this proposed rule and by approving it certifies that it will not have a significant economic impact on a substantial number of small entities. The purpose of this rule is to remove [123I]ioflupane from the list of schedules of the CSA. This action will remove regulatory controls and administrative, civil, and criminal sanctions applicable to controlled substances for handlers and proposed handlers of [123I]ioflupane. Accordingly, it has the potential for some economic impact in the form of cost savings.

If finalized, the proposed rule will affect all persons who would handle, or propose to handle, [123I]ioflupane. Due to the wide variety of unidentifiable and

unquantifiable variables that potentially could influence the distribution and administration rates of new molecular entities, the DEA is unable to determine the number of entities and small entities which might handle [123I]ioflupane.

Although the DEA does not have a reliable basis to estimate the number of affected entities and quantify the economic impact of this proposed rule, a qualitative analysis indicates that, if finalized, this rule is likely to result in some cost savings for the healthcare industry. The affected entities will continue to meet existing Federal and/or state requirements applicable to those who handle radiopharmaceutical substances, including licensure, security, recordkeeping, and reporting requirements, which in many cases are more stringent than the DEA's requirements. However, the DEA estimates cost savings will be realized from the removal of the administrative, civil, and criminal sanctions for those entities handling or proposing to handle [123I]ioflupane, in the form of saved registration fees, and the elimination of additional physical security, recordkeeping, and reporting requirements.

Because of these facts, this rule will not result in a significant economic impact on a substantial number of small entities.

Unfunded Mandates Reform Act of 1995

On the basis of information contained in the "Regulatory Flexibility Act" section above, the DEA has determined and certifies pursuant to the Unfunded Mandates Reform Act of 1995 (UMRA), 2 U.S.C. 1501 *et seq.*, that this action would not result in any federal mandate that may result "in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100,000,000 or more (adjusted for inflation) in any one year * * *." Therefore, neither a Small Government Agency Plan nor any other action is required under provisions of UMRA.

Paperwork Reduction Act

This action does not impose a new collection of information requirement under the Paperwork Reduction Act, 44 U.S.C. 3501–3521. This action would not impose recordkeeping or reporting requirements on State or local governments, individuals, businesses, or organizations. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

List of Subjects in 21 CFR part 1308

Administrative practice and procedure, Drug traffic control, Reporting and recordkeeping requirements.

For the reasons set out above, 21 CFR part 1308 is proposed to be amended to read as follows:

PART 1308—SCHEDULES OF CONTROLLED SUBSTANCES

■ 1. The authority citation for 21 CFR part 1308 continues to read as follows:

Authority: 21 U.S.C. 811, 812, 871(b), unless otherwise noted.

■ 2. In § 1308.12, revise paragraph (b)(4) to read as follows:

§ 1308.12 Schedule II.

* * * * *

(b) * * *

(4) Coca leaves (9040) and any salt, compound, derivative or preparation of coca leaves (including cocaine (9041) and ecgonine (9180) and their salts, isomers, derivatives and salts of isomers and derivatives), and any salt, compound, derivative, or preparation thereof which is chemically equivalent or identical with any of these substances, except that the substances shall not include:

- (i) Decocainized coca leaves or extraction of coca leaves, which extractions do not contain cocaine or ecgonine; or
- (ii) [123I]ioflupane.

* * * * *

Dated: May 6, 2015.

Michele M. Leonhart,
Administrator.

[FR Doc. 2015–13455 Filed 6–2–15; 8:45 am]

BILLING CODE 4410–09–P

DEPARTMENT OF STATE

22 CFR Parts 120, 123, 125, and 127

[Public Notice 9149]

RIN 1400–AD70

International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

AGENCY: Department of State.

ACTION: Proposed rule.

SUMMARY: As part of the President's Export Control Reform (ECR) initiative, the Department of State proposes to amend the International Traffic in Arms

Regulations (ITAR) to update the definitions of "defense article," "defense services," "technical data," "public domain," "export," and "reexport or retransfer" in order to clarify the scope of activities and information that are covered within these definitions and harmonize the definitions with the Export Administration Regulations (EAR), to the extent appropriate. Additionally, the Department proposes to create definitions of "required," "technical data that arises during, or results from, fundamental research," "release," "retransfer," and "activities that are not exports, reexports, or retransfers" in order to clarify and support the interpretation of the revised definitions that are proposed in this rulemaking. The Department proposes to create new sections detailing the scope of licenses, unauthorized releases of information, and the "release" of secured information, and revises the sections on "exports" of "technical data" to U.S. persons abroad. Finally, the Department proposes to address the electronic transmission and storage of unclassified "technical data" via foreign communications infrastructure. This rulemaking proposes that the electronic transmission of unclassified "technical data" abroad is not an "export," provided that the data is sufficiently secured to prevent access by foreign persons. Additionally, this proposed rule would allow for the electronic storage of unclassified "technical data" abroad, provided that the data is secured to prevent access by parties unauthorized to access such data. The revisions contained in this proposed rule are part of the Department of State's retrospective plan under Executive Order 13563 first submitted on August 17, 2011.

DATES: The Department of State will accept comments on this proposed rule until August 3, 2015.

ADDRESSES: Interested parties may submit comments within 60 days of the date of publication by one of the following methods:

- **Email:** DDTCCPublicComments@state.gov with the subject line, "ITAR Amendment—Revisions to Definitions; Data Transmission and Storage."
- **Internet:** At www.regulations.gov, search for this notice by using this rule's RIN (1400-AD70).

Comments received after that date may be considered, but consideration cannot be assured. Those submitting comments should not include any personally identifying information they do not desire to be made public or information for which a claim of

confidentiality is asserted because those comments and/or transmittal emails will be made available for public inspection and copying after the close of the comment period via the Directorate of Defense Trade Controls Web site at www.pmddtc.state.gov. Parties who wish to comment anonymously may do so by submitting their comments via www.regulations.gov, leaving the fields that would identify the commenter blank and including no identifying information in the comment itself. Comments submitted via www.regulations.gov are immediately available for public inspection.

FOR FURTHER INFORMATION CONTACT: Mr. C. Edward Peartree, Director, Office of Defense Trade Controls Policy, Department of State, telephone (202) 663-1282; email DDTCResponseTeam@state.gov. ATTN: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage. The Department of State's full retrospective plan can be accessed at <http://www.state.gov/documents/organization/181028.pdf>.

SUPPLEMENTARY INFORMATION: The Directorate of Defense Trade Controls (DDTC), U.S. Department of State, administers the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130). The items subject to the jurisdiction of the ITAR, *i.e.*, "defense articles" and "defense services," are identified on the ITAR's U.S. Munitions List (USML) (22 CFR 121.1). With few exceptions, items not subject to the export control jurisdiction of the ITAR are subject to the jurisdiction of the Export Administration Regulations ("EAR," 15 CFR parts 730 through 774, which includes the Commerce Control List (CCL) in Supplement No. 1 to part 774), administered by the Bureau of Industry and Security (BIS), U.S. Department of Commerce. Both the ITAR and the EAR impose license requirements on exports and reexports. Items not subject to the ITAR or to the exclusive licensing jurisdiction of any other set of regulations are subject to the EAR.

BIS is concurrently publishing comparable proposed amendments (BIS companion rule) to the definitions of "technology," "required," "peculiarly responsible," "published," results of "fundamental research," "export," "reexport," "release," and "transfer (in-country)" in the EAR. A side-by-side comparison on the regulatory text proposed by both Departments is available on both agencies' Web sites: www.pmddtc.state.gov and www.bis.doc.gov.

1. Revised Definition of Defense Article

The Department proposes to revise the definition of "defense article" to clarify the scope of the definition. The current text of § 120.6 is made into a new paragraph (a), into which software is added to the list of things that are a "defense article" because software is being removed from the definition of "technical data." This is not a substantive change.

A new § 120.6(b) is added to list those items that the Department has determined should not be a "defense article," even though they would otherwise meet the definition of "defense article." All the items described were formerly excluded from the definition of "technical data" in § 120.10. These items are declared to be not subject to the ITAR to parallel the EAR concept of "not subject to the EAR" as part of the effort to harmonize the ITAR and the EAR. This does not constitute a change in policy regarding these items or the scope of items that are defense articles.

2. Revised Definition of Technical Data

The Department proposes to revise the definition of "technical data" in ITAR § 120.10 in order to update and clarify the scope of information that may be captured within the definition. Paragraph (a)(1) of the revised definition defines "technical data" as information "required" for the "development," "production," operation, installation, maintenance, repair, overhaul, or refurbishing of a "defense article," which harmonizes with the definition of "technology" in the EAR and the Wassenaar Arrangement. This is not a change in the scope of the definition, and additional words describing activities that were in the prior definition are included in parentheses to assist exporters.

Paragraph (a)(1) also sets forth a broader range of examples of formats that "technical data" may take, such as diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, or electronic media, that may constitute "technical data." Additionally, the revised definition includes certain conforming changes intended to reflect the revised and newly added defined terms proposed elsewhere in this rule.

The proposed revised definition also includes a note clarifying that the modification of the design of an existing item creates a new item and that the "technical data" for the modification is "technical data" for the new item.

Paragraph (a)(2) of the revised definition defines "technical data" as

also including information that is enumerated on the USML. This will be "technical data" that is positively described, as opposed to "technical data" described in the standard catch-all "technical data" control for all "technical data" directly related to a "defense article" described in the relevant category. The Department intends to enumerate certain controlled "technical data" as it continues to move the USML toward a more positive control list.

Paragraph (a)(3) of the revised definition defines "technical data" as also including classified information that is for the "development," "production," operation, installation, maintenance, repair, overhaul, or refurbishing of a "defense article" or a 600 series item subject to the EAR. Paragraph (a)(5) of the revised definition defines "technical data" as also including information to access secured "technical data" in clear text, such as decryption keys, passwords, or network access codes. In support of the latter change, the Department also proposes to add a new provision to the list of violations in § 127.1(b)(4) to state that any disclosure of these decryption keys or passwords that results in the unauthorized disclosure of the "technical data" or software secured by the encryption key or password is a violation and will constitute a violation to the same extent as the "export" of the secured information. For example, the "release" of a decryption key may result in the unauthorized disclosure of multiple files containing "technical data" hosted abroad and could therefore constitute a violation of the ITAR for each piece of "technical data" on that server.

Paragraph (b) of the revised definition of "technical data" excludes non-proprietary general system descriptions, information on basic function or purpose of an item, and telemetry data as defined in Note 3 to USML Category XV(f) (§ 121.1). Items formerly identified in this paragraph, principles taught in schools and "public domain" information, have been moved to the new ITAR § 120.6(b).

The proposed definition removes software from the definition of "technical data." Specific and catch-all controls on software will be added elsewhere throughout the ITAR as warranted, as it will now be defined as a separate type of "defense article."

3. Proposed Definition of Required

The Department proposes a definition of "required" in a new § 120.46. "Required" is used in the definition of "technical data" and has, to this point,

been an undefined term in the ITAR. The word is also used in the controls on technology in both the EAR and the Wassenaar Arrangement, as a defined term, which the Department is now proposing to adopt:

... [O]nly that portion of [technical data] that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required [technical data] may be shared by different products.

The proposed definition of "required" contains three notes. These notes explain how the definition is to be applied.

Note 1 provides that the definition explicitly includes information for meeting not only controlled performance levels, but also characteristics and functions. All items described on the USML are identified by a characteristic or function. Additionally, some descriptions include a performance level. As an example, USML Category VIII(a)(1) controls aircraft that are "bombers" and contains no performance level. The characteristic of the aircraft that is controlled is that it is a bomber, and therefore, any "technical data" peculiar to making an aircraft a bomber is "required."

Note 2 states that, with the exception of "technical data" specifically enumerated on the USML, the jurisdictional status of unclassified "technical data" is the same as that of the commodity to which it is directly related. Specifically, it explains that "technical data" for a part or component of a "defense article" is directly related to that part or component, and if the part or component is subject to the EAR, so is the "technical data."

Note 3 establishes a test for determining if information is peculiarly responsible for meeting or achieving the controlled performance levels, characteristics or functions of a "defense article." It uses the same catch-and-release concept that the Department implemented in the definition of "specially designed." It has a similarly broad catch of all information used in or for use in the "development," "production," operation, installation, maintenance, repair, overhaul, or refurbishing of a "defense article." It has four releases that mirror the "specially designed" releases, and one reserved paragraph for information that the Department determines is generally insignificant. The first release is for information identified in a commodity jurisdiction determination. The second release is reserved. The third release is for information that is identical to information used in a non-defense

article that is in "production," and not otherwise enumerated on the ITAR. The fourth release is for information that was developed with knowledge that it is for both a "defense article" and a non-defense article. The fifth release is information that was developed for general purpose commodities.

In the companion rule, BIS proposes to make Note 3 into a stand-alone definition for "peculiarly responsible" as it has application outside of the definition of "required." The substance of Note 3 and the BIS definition of "peculiarly responsible" are identical. DDTTC asks for comments on the placement of this concept.

4. Proposed Definitions of Development and Production

The Department proposes to add § 120.47 for the definition of "development" and § 120.48 for the definition of "production." These definitions are currently in Notes 1 and 2 to paragraph (b)(3) in § 120.41, the definition of "specially designed." Because "technical data" is now defined, in part, as information "required" for the "development" or "production" of a "defense article," and these words are now used in the definition of a "defense service," it is appropriate to define these terms. The adoption of these definitions is also done for the purpose of harmonization because these definitions are also used in the EAR and by the Wassenaar Arrangement.

5. Revised Definition of Public Domain

The Department proposes to revise the definition of "public domain" in ITAR § 120.11 in order to simplify, update, and introduce greater versatility into the definition. The existing version of ITAR § 120.11 relies on an enumerated list of circumstances through which "public domain" information might be published. The Department believes that this definition is unnecessarily limiting in scope and insufficiently flexible with respect to the continually evolving array of media, whether physical or electronic, through which information may be disseminated.

The proposed definition is intended to identify the characteristics that are common to all of the enumerated forms of publication identified in the current rule—with the exception of ITAR § 120.11(a)(8), which is addressed in a new definition for "technical data that arises during, or results from, fundamental research"—and to present those common characteristics in a streamlined definition that does not require enumerated identification

within the ITAR of every current or future qualifying publication scenario. Additionally, the proposed definition incorporates phrases such as “generally accessible” and “without restriction upon its further dissemination” in order to better align the definition found in the EAR and more closely aligned with the definition in the Wassenaar Arrangement control lists.

The proposed definition requires that information be made available to the public without restrictions on its further dissemination. Any information that meets this definition is “public domain.” The definition also retains an exemplary list of information that has been made available to the public without restriction and would be considered “public domain.” These include magazines, periodicals and other publications available as subscriptions, publications contained in libraries, information made available at a public conference, meeting, seminar, trade show, or exhibition, and information posted on public Web sites. The final example deems information that is submitted to co-authors, editors, or reviewers or conference organizers for review for publication to be “public domain,” even prior to actual publication. The relevant restrictions do not include copyright protections or generic property rights in the underlying physical medium.

Paragraph (b) of the revised definition explicitly sets forth the Department’s requirement of authorization to release information into the “public domain.” Prior to making available “technical data” or software subject to the ITAR, the U.S. government must approve the release through one of the following: (1) The Department; (2) the Department of Defense’s Office of Security Review; (3) a relevant U.S. government contracting authority with authority to allow the “technical data” or software to be made available to the public, if one exists; or (4) another U.S. government official with authority to allow the “technical data” or software to be made available to the public.

The requirements of paragraph (b) are not new. Rather, they are a more explicit statement of the ITAR’s requirement that one must seek and receive a license or other authorization from the Department or other cognizant U.S. government authority to release ITAR controlled “technical data,” as defined in § 120.10. A release of “technical data” may occur by disseminating “technical data” at a public conference or trade show, publishing “technical data” in a book or journal article, or posting “technical data” to the Internet. This proposed provision will enhance

compliance with the ITAR by clarifying that “technical data” may not be made available to the public without authorization. Persons who intend to discuss “technical data” at a conference or trade show, or to publish it, must ensure that they obtain the appropriate authorization.

Information that is excluded from the definition of “defense article” in the new § 120.6(b) is not “technical data” and therefore does not require authorization prior to release into the “public domain.” This includes information that arises during or results from “fundamental research,” as described in the new § 120.49; general scientific, mathematical, or engineering principles commonly taught in schools, and information that is contained in patents.

The Department also proposes to add a new provision to § 127.1 in paragraph (a)(6) to state explicitly that the further dissemination of “technical data” or software that was made available to the public without authorization is a violation of the ITAR, if, and only if, it is done with knowledge that the “technical data” or software was made publicly available without an authorization described in ITAR § 120.11(b)(2). Dissemination of publicly available “technical data” or software is not an export-controlled event, and does not require authorization from the Department, in the absence of knowledge that it was made publicly available without authorization.

“Technical data” and software that is made publicly available without proper authorization remains “technical data” or software and therefore remains subject to the ITAR. As such, the U.S. government may advise a person that the original release of the “technical data” or software was unauthorized and put that person on notice that further dissemination would violate the ITAR.

6. Proposed Definition of Technical Data That Arises During, or Results From, Fundamental Research

The Department proposes to move “fundamental research” from the definition of “public domain” in ITAR § 120.11(a)(8) and define “technical data that arises during, or results from, fundamental research” in a new ITAR § 120.49. The Department believes that information that arises during, or results from fundamental research is conceptually distinguishable from the information that would be captured in the revised definition of “public domain” that is proposed in this rule. Accordingly, the Department proposes to address this concept with its own definition. The new definition of

“technical data that arises during, or results from, fundamental research” is consistent with the prior ITAR § 120.11(a)(8), except that the Department has expanded the scope of eligible research to include research that is funded, in whole or in part, by the U.S. government.

7. Revised Definition of Export

The Department proposes to revise the definition of “export” in ITAR § 120.17 to better align with the EAR’s revised definition of the term and to remove activities associated with a defense article’s further movement or release outside the United States, which will now fall within the definition of “reexport” in § 120.19. The definition is revised to explicitly identify that ITAR §§ 126.16 and 126.17 (exemptions pursuant to the Australia and UK Defense Trade Cooperation Treaties) have their own definitions of “export,” which apply exclusively to those exemptions. It also explicitly references the new § 120.49, “Activities that are Not Exports, Reexports, or Retransfers,” which excludes from ITAR control certain transactions identified therein.

Paragraph (a)(1) is revised to parallel the definition of “export” in proposed paragraph (a)(1) of § 734.13 of the EAR. Although the wording has changed, the scope of the control is the same. The provision excepting travel outside of the United States by persons whose personal knowledge includes “technical data” is removed, but the central concept is unchanged. The “release” of “technical data” to a foreign person while in the United States or while travelling remains a controlled event.

Paragraph (a)(2) includes the control listed in the current § 120.17(a)(4) (transfer of technical data to a foreign person). The proposed revisions replace the word “disclosing” with “releasing,” and the paragraph is otherwise revised to parallel proposed paragraph (a)(2) of § 734.13 of the EAR. “Release” is a newly defined concept in § 120.50 that encompasses the previously undefined term “disclose.”

Paragraph (a)(3) includes the control listed in the current § 120.17(a)(2) (transfer of registration, control, or ownership to a foreign person of an aircraft, vessel, or satellite). It is revised to parallel proposed paragraph (a)(3) of § 734.13 of the EAR.

Paragraph (a)(4) includes the control listed in the current § 120.17(a)(3) (transfer in the United States to foreign embassies).

Paragraph (a)(5) maintains the control on performing a “defense service.”

Paragraph (a)(6) is added for the “release” or transfer of decryption keys,

passwords, and other items identified in the new paragraph (a)(5) of the revised definition of "technical data" in § 120.10. This paragraph makes "release" or transfer of information securing "technical data" an "export." Making the release of decryption keys and other information securing technical data in an inaccessible or unreadable format an export allows the Department to propose that providing someone with encrypted "technical data" would not be an "export," under certain circumstances. Provision of a decryption key or other information securing "technical data" is an "export" regardless of whether the foreign person has already obtained access to the secured "technical data." Paragraph (a)(6) of the definitions of export and reexport in this rule and the BIS companion rule present different formulations for this control and the agencies request input from the public on which language more clearly describes the control. The agencies intend, however, that the act of providing physical access to unsecured "technical data" (subject to the ITAR) will be a controlled event. The mere act of providing access to unsecured technology (subject to the EAR) will not, however, be a controlled event unless it is done with "knowledge" that such provision will cause or permit the transfer of controlled "technology" in clear text or "software" to a foreign national.

Paragraph (a)(7) is added for the release of information to a public network, such as the Internet. This makes more explicit the existing control in (a)(4), which includes the publication of "technical data" to the Internet due to its inherent accessibility by foreign persons. This means that before posting information to the Internet, you should determine whether the information is "technical data." You should review the USML, and if there is doubt about whether the information is "technical data," you may request a commodity jurisdiction determination from the Department. If so, a license or other authorization, as described in § 120.11(b), will generally be required to post such "technical data" to the Internet. Posting "technical data" to the Internet without a Department or other authorization is a violation of the ITAR even absent specific knowledge that a foreign national will read the "technical data."

Paragraph (b)(1) is added to clarify existing ITAR controls to explicitly state that disclosing "technical data" to a foreign person is deemed to be an "export" to all countries in which the

foreign person has held citizenship or holds permanent residency.

8. Revised Definition of Reexport

The Department proposes to revise the definition of "reexport" in ITAR § 120.19 to better align with the EAR's revised definition and describe transfers of items subject to the jurisdiction of the ITAR between two foreign countries.

The activities identified are the same as those in paragraphs (a)(1) through (4) of the revised definition of "export," except that the shipment, release or transfer is between two foreign countries or is to a third country national foreign person outside of the United States.

9. Proposed Definition of Release

The Department proposes to add § 120.50, the definition of "release." This term is added to harmonize with the EAR, which has long used the term to cover activities that disclose information to foreign persons. "Release" includes the activities encompassed within the undefined term "disclose." The activities that are captured include allowing a foreign person to inspect a "defense article" in a way that reveals "technical data" to the foreign persons and oral or written exchanges of "technical data" with a foreign person. The adoption of the definition of "release" does not change the scope of activities that constitute an "export" and other controlled transactions under the ITAR.

10. Proposed Definition of Retransfer

The Department proposes to add § 120.51, the definition of "retransfer." "Retransfer" is moved out of the definition of "reexport" in § 120.19 to better harmonize with the EAR, which controls "exports," "reexports" and "transfers (in country)" as discrete events. Under this new definition, a "retransfer" occurs with a change of end use or end user within the same foreign territory. Certain activities may fit within the definition of "reexport" and "retransfer," such as the disclosure of "technical data" to a third country national abroad. Requests for both "reexports" and "retransfers" of "defense articles" will generally be processed through a General Correspondence or an exemption.

11. Proposed Activities That Are Not Exports, Reexports, or Retransfers

The Department proposes to add § 120.52 to describe those "activities that are not exports, reexports, or retransfers" and do not require authorization from the Department. It is not an "export" to launch items into

space, provide "technical data" or software to U.S. persons while in the United States, or move a "defense article" between the states, possessions, and territories of the United States. The Department also proposes to add a new provision excluding from ITAR licensing requirements the transmission and storage of encrypted "technical data" and software.

The Department recognizes that ITAR-controlled "technical data" may be electronically routed through foreign servers unbeknownst to the original sender. This presents a risk of unauthorized access and creates a potential for inadvertent ITAR violations. For example, email containing "technical data" may, without the knowledge of the sender, transit a foreign country's Internet service infrastructure en route to its intended and authorized final destination. Any access to this data by a foreign person would constitute an unauthorized "export" under ITAR § 120.17. Another example is the use of mass data storage (*i.e.*, "cloud storage"). In this case, "technical data" intended to be resident in cloud storage may, without the knowledge of the sender, be physically stored on a server or servers located in a foreign country or multiple countries. Any access to this data, even if unintended by the sender, would constitute an "export" under ITAR § 120.17.

The intent of the proposed ITAR § 120.52(a)(4) is to clarify that when unclassified "technical data" transits through a foreign country's Internet service infrastructure, a license or other approval is not mandated when such "technical data" is encrypted prior to leaving the sender's facilities and remains encrypted until received by the intended recipient or retrieved by the sender, as in the case of remote storage. The encryption must be accomplished in a manner that is certified by the U.S. National Institute for Standards and Technology (NIST) as compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2). Additionally, the Department proposes that the electronic storage abroad of "technical data" that has been similarly encrypted would not require an authorization, so long as it is not stored in a § 126.1 country or in the Russian Federation. This will allow for cloud storage of encrypted data in foreign countries, so long as the "technical data" remains continuously encrypted while outside of the United States.

12. Revised Exemption for the Export of Technical Data for U.S. Persons Abroad

The Department proposes to revise § 125.4(b)(9) to better harmonize controls on the "release" of controlled information to U.S. persons abroad and to update the provisions. The most significant update is that foreign persons authorized to receive "technical data" in the United States will be eligible to receive that same "technical data" abroad, when on temporary assignment on behalf of their employer. The proposed revisions clarify that a person going abroad may use this exemption to "export" "technical data" for their own use abroad. The proposed revisions also clarify that the "technical data" must be secured while abroad to prevent unauthorized "release." It has been long-standing Department practice to hold U.S. persons responsible for the "release" of "technical data" in their possession while abroad. However, given the nature of "technical data" and the proposed exception from licensing for transmission of secured "technical data," the Department has determined it is necessary to implement an affirmative obligation to secure data while abroad.

13. Proposed Scope of License

The Department proposes to add § 123.28 to clarify the scope of a license, in the absence of a proviso, and to state that authorizations are granted based on the information provided by the applicant. This means that while providing false information to the U.S. government as part of the application process for the "export," "reexport," or "retransfer" of a "defense article" is a violation of the ITAR, it also may void the license.

14. Revised Definition of Defense Service

Proposed revisions of the "defense service" definition were published on April 13, 2011, RIN 1400-AC80 (*see* "International Traffic in Arms Regulations: Defense Services," 76 FR 20590) and May 24, 2013 (*see* 78 FR 31444, RIN 1400-AC80). In those rules, the Department explained its determination that the scope of the current definition is overly broad, capturing certain forms of assistance or services that no longer warrant ITAR control.

The Department reviewed comments on that first proposed definition and, when the recommended changes added to the clarity of the regulation, the Department accepted them. For the Department's evaluation of those public comments and recommendations regarding the April 13, 2011, proposed

rule (the first revision), *see* 78 FR 31444, May 24, 2013. The Department's evaluation of the written comments and recommendations in response to the May 24, 2013 proposed rule (the second revision) follows.

Parties commenting on the second revision expressed concern that the definition of "defense service" in paragraph (a)(1) was premised on the use of "other than public domain information." The observation was made that with the intent of removing from the definition of a "defense service" the furnishing of assistance using "public domain" information, but not basing the assistance on the use of "technical data," the Department was continuing to require the licensing of activities akin to those that were based on the use of "public domain" information. The Department has fully revised paragraph (a)(1) to remove the use of the "other than public domain information" or "technical data" from the determination of whether an activity is a "defense service." Furthermore, the Department has added a new provision declaring that the activities described in paragraph (a)(1) are not a "defense service" if performed by a U.S. person or foreign person in the United States who does not have knowledge of U.S.-origin "technical data" directly related to the "defense article" that is the subject of the assistance or training or another "defense article" described in the same USML paragraph prior to performing the service. A note is added to clarify that a person will be deemed to have knowledge of U.S.-origin "technical data" if the person previously participated in the "development" of a "defense article" described in the same USML paragraph, or accessed (physically or electronically) that "technical data." A note is also added to clarify that those U.S. persons abroad who only received U.S.-origin "technical data" as a result of their activities on behalf of a foreign person are not included within the scope of paragraph (a)(1). A third note is added to clarify that DDTC-authorized foreign person employees in the United States who provide "defense services" on behalf of their U.S. employer are considered to be included with the U.S. employer's authorization, and need not be listed on the U.S. employer's technical assistance agreement or receive a separate authorization for those services. The Department also removed the activities of design, development, and engineering from paragraph (a)(1) and moved them to paragraph (a)(2).

Commenting parties recommended revising paragraph (a)(1) to remove the

provision of "technical data" as a "defense service," because there are already licensing requirements for the "export" of "technical data." The Department confirms that it eliminated from the definition of a "defense service" the act of furnishing "technical data" to a foreign person. Such activity still constitutes an "export" and would require an ITAR authorization. New paragraph (a)(1) is concerned with the furnishing of assistance, whereas the "export" of "technical data" alone, without the furnishing of assistance, is not a "defense service." The "export" of "technical data" requires an authorization (Department of State form DSP-5 or DSP-85) or the use of an applicable exemption.

Commenting parties recommended the definition be revised to explicitly state that it applies to the furnishing of assistance by U.S. persons, or by foreign persons in the United States. The Department partially accepted this recommendation. However, the Department notes that ITAR § 120.1(c) provides that only U.S. persons and foreign governmental entities in the United States may be granted a license or other approval pursuant to the ITAR, and that foreign persons may only receive a "reexport" or "retransfer" approval or approval for brokering activities. Therefore, approval for the performance of a defense service in the United States by a foreign person must be obtained by a U.S. person, such as an employer, on behalf of the foreign person. Regarding a related recommendation, the Department also notes that the furnishing of a type of assistance described by the definition of a "defense service" is not an activity within the Department's jurisdiction when it is provided by a foreign person outside the United States to another foreign person outside the United States on a foreign "defense article" using foreign-origin "technical data."

In response to commenting parties, the Department specified that the examples it provided for activities that are not "defense services" are not exhaustive. Rather, they are provided to answer the more frequent questions the Department receives on the matter. The Department removed these examples from paragraph (b) and included them as a note to paragraph (a).

A commenting party recommended that paragraphs (a)(5) and (a)(6), regarding the furnishing of assistance in the integration of a spacecraft to a launch vehicle and in the launch failure analysis of a spacecraft or launch vehicle, respectively, be removed, and that those activities be described in the USML categories covering spacecraft

and launch vehicles, on the basis that a general definition should not have such program-specific clauses. As discussed in the May 13, 2014 interim final rule revising USML Category XV (79 FR 27180), the Department accepted this recommendation and revised paragraph (f) of USML Category XV and paragraph (i) of USML Category IV accordingly. The revision includes the recommendation of commenting parties to specifically provide that the service must be provided to a foreign person in order for it to be a licensable activity.

Commenting parties recommended the Department define the term "tactical employment," so as to clarify what services would be captured by paragraph (a)(3). The Department determined that employment of a "defense article" should remain a controlled event, due to the nature of items now controlled in the revised USML categories. After ECR, those items that remain "defense articles" are the most sensitive and militarily critical equipment that have a significant national security or intelligence application. Allowing training and other services to foreign nationals in the employment of these "defense articles" without a license would not be appropriate. Therefore, the Department removed the word "tactical" and converted the existing exemption for basic operation of a "defense article," authorized by the U.S. government for "export" to the same recipient, into an exclusion from paragraph (a)(3).

A commenting party recommended the Department address the instance of the integration or installation of a "defense article" into an item, much as it addressed the instance of the integration or installation of an item into a "defense article." Previously, the Department indicated this would be the subject of a separate rule, and addressed the "export" of such items in a proposed rule (*see* 76 FR 13928), but upon review the Department accepted this recommendation, and revised paragraph (a)(2), the note to paragraph (a)(2), and the note to paragraph (a) accordingly. In addition, the Department has changed certain terminology used in the paragraph: instead of referring to the "transfer" of "technical data," the paragraph is premised on the "use" of "technical data." This change is consistent with removing from the definition of a "defense service" the furnishing of "technical data" to a foreign person when there is not also the furnishing of assistance related to that "technical data."

A commenting party requested clarification of the rationale behind

selectively excepting from the "defense services" definition the furnishing of services using "public domain" information. The Department did so in paragraph (a)(1), and now excludes those services performed by U.S. persons who have not previously had access to any U.S. origin "technical data" on the "defense article" being serviced. In contrast, the Department did not do so in paragraphs (a)(2) and (a)(3) and former paragraphs (a)(5) and (a)(6). In the case of paragraph (a)(2), the rationale for not doing so is that the activities involved in the development of a "defense article," or in integrating a "defense article" with another item, inherently involve the advancement of the military capacity of another country and therefore constitute activities over which the U.S. government has significant national security and foreign policy concerns. To the extent that an activity listed in paragraph (a)(1), such as modification or testing, is done in the "development" of a "defense article," such activities constitute "development" and are within the scope of paragraph (a)(2). With regard to paragraph (a)(3), the furnishing of assistance (including training) in the employment of a "defense article" is a type of activity that the Department believes warrants control as a "defense service," due to the inherently military nature of providing training and other services in the employment of a "defense article" (changes to paragraph (a)(3) are described above). The services described in former paragraphs (a)(5) and (a)(6) (and now in USML Categories IV(i) and XV(f)) are pursuant to Public Law 105-261.

A commenting party recommended limiting paragraph (a)(2) to the integration of ECCN 9A515 and 600 series items into defense articles, saying that the regulations should focus on items subject to the EAR with a military or space focus. The Department's focus with this provision is in fact the "defense article." Items that are to be integrated with a "defense article," which may not themselves be defense articles, may be beyond the authority of the Department to regulate. The Department did not accept this recommendation.

A commenting party recommended limiting the definition of integration to changes in the function of the "defense article," and to exclude modifications in fit. For the purposes of illustration, this commenting party used one of the examples provided by the Department in the note to paragraph (a)(2): The manufacturer of the military vehicle will need to know the dimensions and electrical requirements of the dashboard

radio when designing the vehicle. In this instance, paragraph (a)(2) would not apply, as this example addresses the manufacture of a "defense article," which is covered by paragraph (a)(1). If the radio to be installed in this vehicle is subject to the EAR, the provision to the manufacturer of information regarding the radio is not within the Department's licensing jurisdiction. In an instance of a service entailing the integration of an item with a "defense article," where there would be modification to any of the items, the Department believes such assistance would inherently require the use of "technical data." Therefore, this exclusion would be unacceptably broad. However, the Department has accepted the recommendation to clarify the definition and exclude changes to fit to any of the items involved in the integration activity, provided that such services do not entail the use of "technical data" directly related to the "defense article." Upon review, changes to fit are not an aspect of integration, which is the "engineering analysis needed to unite a 'defense article' and one or more items," and therefore are not captured in paragraph (a)(2). The modifications of the "defense article" to accommodate the fit of the item to be integrated, which are within the activity covered by installation, are only those modifications to the "defense article" that allow the item to be placed in its predetermined location. Any modifications to the design of a "defense article" are beyond the scope of installation. Additionally, while minor modifications may be made to a "defense article" without the activity being controlled under (a)(2) as an integration activity, all modifications of defense articles, regardless of sophistication, are activities controlled under (a)(1) if performed by someone with prior knowledge of U.S.-origin "technical data." "Fit" is defined in ITAR § 120.41: "The fit of a commodity is defined by its ability to physically interface or connect with or become an integral part of another commodity" (*see*, Note 4 to paragraph (b)(3)).

Commenting parties recommended revising paragraph (a)(2) to provide that such assistance described therein would be a "defense service" only if U.S.-origin "technical data" is exported. The law and regulations do not mandate this limitation. Section 38 of the Arms Export Control Act provides that the President is authorized to control the "export" of defense articles and defense services. The ITAR, in defining "defense article," "technical data," and "export," does not provide the qualifier "U.S.-

origin" (see ITAR §§ 120.6, 120.10, and 120.17, respectively). In the instance described by the commenting party, of the integration of a commercial item into a foreign-origin "defense article," the Department retains jurisdiction when the service is provided by a U.S. person.

A commenting party recommended revising paragraph (a)(2) so that the paragraph (a)(1) exception of the furnishing of assistance using "public domain" information is not nullified by paragraph (a)(2), as most of the activities described in paragraph (a)(1) involve integration as defined in the note to paragraph (a)(2). The Department believes each of the activities described in paragraphs (a)(1) and (a)(2) are sufficiently well defined to distinguish them one from the other. Therefore, the Department does not agree that paragraph (a)(2) nullifies the intention of paragraph (a)(1), and does not accept this recommendation.

A commenting party requested clarification that providing an item subject to the EAR for the purposes of integration into a "defense article" is not a "defense service." The provision of the item in this instance, unaccompanied by assistance in the integration of the item into a "defense article," is not within the scope of "the furnishing of assistance," and therefore is not a defense service.

Commenting parties recommended clarification on whether the servicing of an item subject to the EAR that has been integrated with a "defense article" would be a "defense service." The Department notes that such activity is not a "defense service," provides it as an example of what is not a "defense service" in the note to paragraph (a), and also notes that it would be incumbent on the applicant to ensure that in providing this service, "technical data" directly related to the "defense article" is not used.

Commenting parties expressed concern over the potential negative effect of paragraph (a)(2) and the definition in general on university-based educational activities and scientific communication, and recommended clarification of the relationship between the definition of "defense services" and the exemption for the "export" of "technical data" at ITAR § 125.4(b)(10). Disclosures of "technical data" to foreign persons who are bona-fide and full time regular employees of universities continue to be exports for which ITAR § 125.4(b)(10) is one licensing exemption. The Department believes that, in most cases, the normal duties of a university employee do not encompass the

furnishing of assistance to a foreign person, in the activities described in paragraph (a). Therefore, in the context of employment with the university, the Department does not perceive that the foreign person's use of the "technical data" would be described by ITAR § 120.9(a)(2), or any part of paragraph (a).

In response to the recommendation of one commenting party, the Department added a note clarifying that the installation of an item into a "defense article" is not a "defense service," provided no "technical data" is used in the rendering of the service.

A commenting party recommended clarification of the licensing process for the "export" of an EAR 600 series item that is to be integrated into a "defense article." The Department of Commerce has "export" authority over the 600 series item, and the exporter must obtain a license from the Department of Commerce, if necessary. The exporter must also obtain an approval from the Department of State to provide any "defense service," including integration assistance pursuant to paragraph (a)(2).

A commenting party recommended removing "testing" as a type of "defense service," stating it was not included in the definition of "organizational-level maintenance." In including testing as part of the former definition but not of the latter, the Department does not perceive an inconsistency or conflict. To the extent that certain testing is within the definition of organization-level maintenance, that testing is explicitly excluded, as organizational-level maintenance is not covered under the definition of a "defense service." However, all other testing remains a "defense service." The Department intends for the furnishing of assistance to a foreign person, whether in the United States or abroad, in the testing of defense articles to be an activity requiring Department approval under the conditions of paragraph (a)(1). The Department did not accept this recommendation.

Commenting parties provided recommendations for revising the definitions of "public domain" information and "technical data." Those definitions are proposed in this rule as well. To the extent that evaluation of the proposed changes to "defense services" hinges on these terms, the Department invites commenting parties to submit analyses of the impact of these revised definitions on the revised "defense service" definition in this proposed rule.

Commenting parties recommended clarification of the regulation regarding the furnishing of assistance and training

in organizational-level (basic-level) maintenance. The Department harmonized paragraph (a)(1) and the example regarding organizational-level maintenance by revising the Note to Paragraph (a), which sets forth activities that are not "defense services," so that it specifically provides that "the furnishing of assistance (including training) in organizational-level (basic-level) maintenance of a defense article" is an example of an activity that is not a defense service.

In response to commenting parties, the Department clarifies that the example of employment by a foreign person of a natural U.S. person as not constituting a "defense service" is meant to address, among other scenarios, the instance where such a person is employed by a foreign defense manufacturer, but whose employment in fact does not entail the furnishing of assistance as described in ITAR § 120.9(a). By "natural person," the Department means a human being, as may be inferred from the definition of "person" provided in ITAR § 120.14.

In response to the recommendation of a commenting party, the Department confirms that, as stated in a Department of Commerce notice, "Technology subject to the EAR that is used with technical data subject to the ITAR that will be used under the terms of a Technical Assistance Agreement (TAA) or Manufacturing License Agreement (MLA) and that would otherwise require a license from [the Department of Commerce] may all be exported under the TAA or MLA" (see 78 FR 22660). In DDTC publication *Guidelines for Preparing Electronic Agreements (Revision 4.2)*, Section 20.1.d., the following conditions are stipulated: The technology subject to the EAR will be used with "technical data" subject to the ITAR and described in the agreement, and the technology subject to the EAR will be used under the terms of a TAA or MLA (see <http://www.pmddtc.state.gov/licensing/agreement.html>).

Request for Comments

The Department invites public comment on any of the proposed definitions set forth in this rulemaking. With respect to the revisions to ITAR § 120.17, the Department recognizes the increasingly complex nature of telecommunications infrastructure and the manner in which data is transmitted, stored, and accessed, and accordingly seeks public comment with special emphasis on: (1) How adequately the proposed regulations address the technical aspects of data transmission and storage; (2) whether

the proposed regulations mitigate unintended or unauthorized access to transmitted or stored data; and (3) whether the proposed regulations impose an undue financial or compliance burden on the public.

The public is also asked to comment on the effective date of the final rule. Export Control Reform rules that revised categories of the USML and created new 600 series ECCN have had a six-month delayed effective date to allow for exporters to update the classification of their items. In general, rules effecting export controls have been effective on the date of publication, due to the impact on national security and foreign policy. As this proposed rule and the companion proposed rule from the Bureau of Industry and Security revise definitions within the ITAR and the EAR and do not make any changes to the USML or CCL, the Department proposes (should the proposed rule be adopted) a 30-day delayed effective date to allow exporters to ensure continued compliance.

Regulatory Analysis and Notices

Administrative Procedure Act

The Department of State is of the opinion that controlling the import and export of defense articles and services is a foreign affairs function of the U.S. government and that rules implementing this function are exempt from sections 553 (rulemaking) and 554 (adjudications) of the Administrative Procedure Act (APA). Although the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of the APA, the Department is publishing this rule with a 60-day provision for public comment and without prejudice to its determination that controlling the import and export of defense services is a foreign affairs function.

Regulatory Flexibility Act

Since the Department is of the opinion that this proposed rule is exempt from the rulemaking provisions of 5 U.S.C. 553, there is no requirement for an analysis under the Regulatory Flexibility Act.

Unfunded Mandates Reform Act of 1995

This proposed amendment does not involve a mandate that will result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of \$100 million or more in any year and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the

Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (the "Act"), a major rule is a rule that the Administrator of the OMB Office of Information and Regulatory Affairs finds has resulted or is likely to result in: (1) An annual effect on the economy of \$100,000,000 or more; (2) a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions; or (3) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets.

The Department does not believe this rulemaking will have an annual effect on the economy of \$100,000,000 or more, nor will it result in a major increase in costs or prices for consumers, individual industries, federal, state, or local government agencies, or geographic regions, or have significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and foreign markets. The proposed means of solving the issue of data protection are both familiar to and extensively used by the affected public in protecting sensitive information.

Executive Orders 12372 and 13132

This proposed amendment will not have substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 13132, it is determined that this proposed amendment does not have sufficient federalism implications to require consultations or warrant the preparation of a federalism summary impact statement. The regulations implementing Executive Order 12372 regarding intergovernmental consultation on Federal programs and activities do not apply to this proposed amendment.

Executive Orders 12866 and 13563

Executive Orders 12866 and 13563 direct agencies to assess costs and benefits of available regulatory

alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributed impacts, and equity). The executive orders stress the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This proposed rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, the proposed rule has been reviewed by the Office of Management and Budget (OMB).

Executive Order 12988

The Department of State has reviewed the proposed amendment in light of sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

Executive Order 13175

The Department of State has determined that this rulemaking will not have tribal implications, will not impose substantial direct compliance costs on Indian tribal governments, and will not preempt tribal law. Accordingly, Executive Order 13175 does not apply to this rulemaking.

Paperwork Reduction Act

This rule does not impose any new reporting or recordkeeping requirements subject to the Paperwork Reduction Act, 44 U.S.C. Chapter 35; however, the Department of State seeks public comment on any unforeseen potential for increased burden.

List of Subjects

22 CFR 120 and 125

Arms and munitions, Classified information, Exports.

22 CFR 123

Arms and munitions, Exports, Reporting and recordkeeping requirements.

22 CFR Part 127

Arms and munitions, Exports, Crime, Law, Penalties, Seizures and forfeitures.

Accordingly, for the reasons set forth above, title 22, chapter I, subchapter M, parts 120, 123, 125, and 127 are proposed to be amended as follows:

PART 120—PURPOSE AND DEFINITIONS

■ 1. The authority citation for part 120 continues to read as follows:

Authority: Secs. 2, 38, and 71, Pub. L. 90-629, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2794; 22 U.S.C. 2651a; Pub. L. 105-261, 112 Stat. 1920; Pub. L. 111-266; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

■ 2. Section 120.6 is amended by designating the current text as paragraph (a), revising the first sentence of newly designated paragraph (a), and adding paragraph (b) to read as follows:

§ 120.6 Defense article.

(a) *Defense article* means any item, software, or technical data designated in § 121.1 of this subchapter. * * *

(b) The following are not defense articles and thus not subject to the ITAR:

- (1) [Reserved]
- (2) [Reserved]
- (3) Information and software that:
 - (i) Are in the public domain, as described in § 120.11;
 - (ii) Arise during, or result from, fundamental research, as described in § 120.46;
 - (iii) Concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution; or
 - (iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order.

Note to paragraph (b): Information that is not within the scope of the definition of technical data (see § 120.10) and not directly related to a defense article, or otherwise described on the USML, is not subject to the ITAR.

■ 3. Section 120.9 is revised to read as follows:

§ 120.9 Defense service.

(a) *Defense service* means:

- (1) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the production, assembly, testing, intermediate- or depot-level maintenance (see § 120.38), modification, demilitarization, destruction, or processing of a defense article (see § 120.6), by a U.S. person or foreign person in the United States, who has knowledge of U.S.-origin technical data directly related to the defense article that is the subject of the assistance, prior to performing the service;

Note 1 to paragraph (a)(1): "Knowledge of U.S.-origin technical data" for purposes of paragraph (a)(1) can be established based on all the facts and circumstances. However, a person is deemed to have "knowledge of

U.S.-origin technical data" directly related to a defense article if the person participated in the development of a defense article described in the same USML paragraph or accessed (physically or electronically) technical data directly related to the defense article that is the subject of the assistance, prior to performing the service.

Note 2 to paragraph (a)(1): U.S. persons abroad who only receive U.S.-origin technical data as a result of their activities on behalf of a foreign person are not included within paragraph (a)(1).

Note 3 to paragraph (a)(1): Foreign person employees in the United States providing defense services as part of Directorate of Defense Trade Controls-authorized employment need not be listed on the U.S. employer's technical assistance agreement or receive separate authorization to perform defense services on behalf of their authorized U.S. employer.

(2) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the development of a defense article, or the integration of a defense article with any other item regardless of whether that item is subject to the ITAR or technical data is used;

Note to paragraph (a)(2): "Integration" means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software to enable operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from "installation." Installation means the act of putting an item in its predetermined place without the use of technical data or any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, and there is no use of technical data.). The "fit" of an item is defined by its ability to physically interface or connect with or become an integral part of another item. (see § 120.41).

(3) The furnishing of assistance (including training) to a foreign person (see § 120.16), regardless of whether technical data is used, whether in the United States or abroad, in the employment of a defense article, other than basic operation of a defense article authorized by the U.S. government for export to the same recipient;

(4) Participating in or directing combat operations for a foreign person (see § 120.16), except as a member of the regular military forces of a foreign

nation by a U.S. person who has been drafted into such forces; or

(5) The furnishing of assistance (including training) to the government of a country listed in § 126.1 of this subchapter in the development, production, operation, installation, maintenance, repair, overhaul or refurbishing of a defense article or a part component, accessory or attachments specially designed for a defense article.

Note to paragraph (a): The following are examples of activities that are not defense services:

1. The furnishing of assistance (including training) in organizational-level (basic-level) maintenance (see § 120.38) of a defense article;
2. Performance of services by a U.S. person in the employment of a foreign person, except as provided in this paragraph;
3. Servicing of an item subject to the EAR (see § 120.42) that has been integrated or installed into a defense article, or the servicing of an item subject to the EAR into which a defense article has been installed or integrated, without the use of technical data, except as described in paragraph (a)(5) of this section;
4. The installation of any item into a defense article, or the installation of a defense article into any item;
5. Providing law enforcement, physical security, or personal protective services (including training and advice) to or for a foreign person (if such services necessitate the export of a defense article a license or other approval is required for the export of the defense article, and such services that entail the employment or training in the employment of a defense article are addressed in paragraph (a)(3) of this section);
6. The furnishing of assistance by a foreign person not in the United States;
7. The furnishing of medical, logistical (other than maintenance), translation, financial, legal, scheduling, or administrative services;
8. The furnishing of assistance by a foreign government to a foreign person in the United States, pursuant to an arrangement with the Department of Defense; and
9. The instruction in general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities.

(b) [Reserved]

■ 4. Section 120.10 is revised to read as follows:

§ 120.10 Technical data.

(a) *Technical data* means, except as set forth in paragraph (b) of this section:

- (1) Information required for the development (see § 120.47) (including design, modification, and integration design), production (see § 120.48) (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article. Technical data may be in any tangible or intangible form, such as written or

oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;

Note to paragraph (a)(1): The modification of an existing item creates a new item and technical data for the modification is technical data for the development of the new item.

(2) Information enumerated on the USML (*i.e.*, not controlled pursuant to a catch-all USML paragraph);

(3) Classified information for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article or a 600 series item subject to the EAR;

(4) Information covered by an invention secrecy order; or

(5) Information, such as decryption keys, network access codes, or passwords, that would allow access to other technical data in clear text or software (*see* § 127.1(b)(4) of this subchapter).

(b) *Technical data does not include:*

(1) Non-proprietary general system descriptions;

(2) Information on basic function or purpose of an item; or

(3) Telemetry data as defined in note 3 to USML Category XV(f) (*see* § 121.1 of this subchapter).

■ 5. Section 120.11 is revised to read as follows:

§ 120.11 Public domain.

(a) Except as set forth in paragraph (b) of this section, unclassified information and software are in the public domain, and are thus not technical data or software subject to the ITAR, when they have been made available to the public without restrictions upon their further dissemination such as through any of the following:

(1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;

(2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;

(3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;

(4) Public dissemination (*i.e.*, unlimited distribution) in any form (*e.g.*, not necessarily in published form), including posting on the Internet on sites available to the public; or

(5) Submission of a written composition, manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for publication or presentation.

(b) Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from:

(1) The Directorate of Defense Trade Controls;

(2) The Department of Defense's Office of Security Review;

(3) The relevant U.S. government contracting entity with authority to allow the technical data or software to be made available to the public; or

(4) Another U.S. government official with authority to allow the technical data or software to be made available to the public.

Note 1 to § 120.11: Section 127.1(a)(6) of this subchapter prohibits, without written authorization from the Directorate of Defense Trade Controls, U.S. and foreign persons from exporting, reexporting, retransferring, or otherwise making available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in paragraph (b) of this section.

Note 2 to § 120.11: An export, reexport, or retransfer of technical data or software that was made publicly available by another person without authorization is not a violation of this subchapter, except as described in § 127.1(a)(6) of this subchapter.

■ 6. Section 120.17 is revised to read as follows:

§ 120.17 Export.

(a) Except as set forth in § 120.52, § 126.16, or § 126.17 of this subchapter, *export* means:

(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article outside of the United States in any manner;

(2) Releasing or otherwise transferring technical data or software (source code or object code) to a foreign person in the United States (a "deemed export");

(3) Transferring by a person in the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person;

(4) Releasing or otherwise transferring a defense article to an embassy or to any

agency or subdivision of a foreign government, such as a diplomatic mission, in the United States;

(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad;

(6) Releasing or otherwise transferring information, such as decryption keys, network access codes, passwords, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred; or

(7) Making technical data available via a publicly available network (*e.g.*, the Internet).

(b) Any release in the United States of technical data or software to a foreign person is a deemed export to all countries in which the foreign person has held citizenship or holds permanent residency.

■ 7. Section 120.19 is revised to read as follows:

§ 120.19 Reexport.

(a) Except as set forth in § 120.52, *reexport* means:

(1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;

(2) Releasing or otherwise transferring technical data or software to a foreign person of a country other than the foreign country where the release or transfer takes place (a "deemed reexport");

(3) Transferring by a person outside of the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person outside the United States; or

(4) Releasing or otherwise transferring outside of the United States information, such as decryption keys, network access codes, password, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred.

(b) [Reserved]

§ 120.41 [Amended]

■ 8. Section 120.41 is amended by reserving Note 1 to paragraph (b)(3) and Note 2 to paragraph (b)(3).

■ 9. Section 120.46 is added to read as follows:

§ 120.46 Required.

(a) As applied to technical data, the term *required* refers to only that portion

of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required technical data may be shared by different products.

Note 1 to paragraph (a): The references to "characteristics" and "functions" are not limited to entries on the USML that use specific technical parameters to describe the scope of what is controlled. The "characteristics" and "functions" of an item listed are, absent a specific regulatory definition, a standard dictionary's definition of the item. For example, USML Category VIII(a)(1) controls aircraft that are "bombers." No performance level is identified in the entry, but the characteristic of the aircraft that is controlled is that it is a bomber. Thus, any technical data, regardless of significance, peculiar to making an aircraft a bomber as opposed to, for example, an aircraft controlled under ECCN 9A610.a or ECCN 9A991.a, would be technical data required for a bomber and thus controlled under USML Category VIII(i).

Note 2 to paragraph (a): The ITAR and the EAR often divide within each set of regulations or between each set of regulations:

1. Controls on parts, components, accessories, attachments, and software; and
2. Controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated.

With the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data is the same as the jurisdictional status of the defense article or item subject to the EAR to which it is directly related. Thus, if technology is directly related to the production of an ECCN 9A610.x aircraft component that is to be integrated or installed in a USML Category VIII(a) aircraft, the technology is controlled under ECCN 9E610, not USML Category VIII(i).

Note 3 to paragraph (a): Technical data is "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" if it is used in or for use in the development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article unless:

1. The Department of State has determined otherwise in a commodity jurisdiction determination;
2. [Reserved];
3. It is identical to information used in or with a commodity or software that:
 - i. Is or was in production (*i.e.*, not in development); and
 - ii. Is not a defense article;
4. It was or is being developed with knowledge that it is for or would be for use in or with both defense articles and commodities not on the U.S. Munitions List; or

5. It was or is being developed for use in or with general purpose commodities or software (*i.e.*, with no knowledge that it would be for use in or with a particular commodity).

(b) [Reserved]

■ 10. Section 120.47 is added to read as follows:

§ 120.47 Development.

Development is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. Development includes modification of the design of an existing item.

■ 11. Section 120.48 is added to read as follows:

§ 120.48 Production.

Production means all production stages, such as product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance. This includes "serial production" where commodities have passed production readiness testing (*i.e.*, an approved, standardized design ready for large scale production) and have been or are being produced on an assembly line for multiple commodities using the approved, standardized design.

■ 12. Section 120.49 is added to read as follows:

§ 120.49 Technical data that arises during, or results from, fundamental research.

(a) *Technical Data arising during, or resulting from, fundamental research.* Unclassified information that arises during, or results from, fundamental research and is intended to be published is not technical data when the research is:

- (1) Conducted in the United States at an accredited institution of higher learning located; or
- (2) Funded, in whole or in part, by the U.S. government.

Note 1 to paragraph (a): The inputs used to conduct fundamental research, such as information, equipment, or software, are not "technical data that arises during or results from fundamental research" except to the extent that such inputs are technical data that arose during or resulted from earlier fundamental research.

Note 2 to paragraph (a): There are instances in the conduct of research, whether fundamental, basic, or applied, where a researcher, institution, or company may decide to restrict or protect the release or publication of technical data contained in research results. Once a decision is made to

maintain such technical data as restricted or proprietary, the technical data becomes subject to the ITAR.

(b) *Prepublication review.* Technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data contained in the research without any restriction or delay, including U.S. government-imposed access and dissemination controls or research sponsor proprietary information review.

Note 1 to paragraph (b): Although technical data arising during or resulting from fundamental research is not considered "intended to be published" if researchers accept restrictions on its publication, such technical data will nonetheless qualify as technical data arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

Note 2 to paragraph (b): Research that is voluntarily subjected to U.S. government prepublication review is considered intended to be published for all releases consistent with any resulting controls.

Note 3 to paragraph (b): Technical data resulting from U.S. government funded research which is subject to government-imposed access and dissemination or other specific national security controls qualifies as technical data resulting from fundamental research, provided that all government-imposed national security controls have been satisfied.

(c) *Fundamental research definition.* Fundamental research means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

(1) *Basic research* means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

(2) *Applied research* means the effort that:

(i) Normally follows basic research, but may not be severable from the related basic research;

(ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and

(iii) Attempts to advance the state of the art.

■ 13. Section 120.50 is added to read as follows:

§ 120.50 Release.

(a) Except as set forth in § 120.52, technical data and software are released through:

(1) Visual or other inspection by foreign persons of a defense article that reveals technical data or software to a foreign person; or

(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad.

(b) [Reserved]

■ 14. Section 120.51 is added to read as follows:

§ 120.51 Retransfer.

Except as set forth in § 120.52 of this subchapter, a *retransfer* is a change in end use or end user of a defense article within the same foreign country.

■ 15. Section 120.52 is added to read as follows:

§ 120.52 Activities that are not exports, reexports, or retransfers.

(a) The following activities are not exports, reexports, or retransfers:

(1) Launching a spacecraft, launch vehicle, payload, or other item into space;

(2) While in the United States, releasing technical data or software to a U.S. person;

(3) Shipping, moving, or transferring defense articles between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census; and

(4) Sending, taking, or storing technical data or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications; and

(iv) Not stored in a country proscribed in § 126.1 of this subchapter or the Russian Federation.

(b) For purposes of this section, end-to-end encryption means the provision of uninterrupted cryptographic

protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access technical data or software in encrypted form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such technical data or software.

Note to § 120.52: See § 127.1 of this subchapter for prohibitions on the release or transfer of technical data or software, in any form, to any person with knowledge that a violation will occur.

PART 123—LICENSES FOR THE EXPORT AND TEMPORARY IMPORT OF DEFENSE ARTICLES

■ 16. The authority citation for part 123 continues to read as follows:

Authority: Secs. 2, 38, and 71, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2753; 22 U.S.C. 2651a; 22 U.S.C. 2776; Pub. L. 105-261, 112 Stat. 1920; Sec. 1205(a), Pub. L. 107-228; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

■ 17. Section 123.28 is added to read as follows:

§ 123.28 Scope of a license.

Unless limited by a condition set out in a license, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. DDTC grants licenses in reliance on representations the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted.

PART 124—AGREEMENTS, OFFSHORE PROCUREMENT, AND OTHER DEFENSE SERVICES

■ 18. The authority citation for part 124 continues to read as follows:

Authority: Secs. 2, 38, and 71, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2797); 22 U.S.C. 2651a; 22 U.S.C. 2776; Section 1514, Pub. L. 105-261; Pub. L. 111-266; Section 1261, Pub. L. 112-239; E.O. 13637, 78 FR 16129.

■ 19. Section 124.1 is amended by adding paragraph (e) to read as follows:

§ 124.1 Manufacturing license agreements and technical assistance agreements.

* * * * *

(e) Unless limited by a condition set out in an agreement, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the agreement, license, and any letters of explanation. DDTC approves agreements and grants licenses in reliance on representations the applicant made in or submitted in connection with the agreement, letters of explanation, and other documents submitted.

PART 125—LICENSES FOR THE EXPORT OF TECHNICAL DATA AND CLASSIFIED DEFENSE ARTICLES

■ 20. The authority citation for part 125 continues to read as follows:

Authority: Secs. 2 and 38, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778); 22 U.S.C. 2651a; E.O. 13637, 78 FR 16129.

■ 21. Section 125.4 is amended by revising paragraph (b)(9) to read as follows:

§ 125.4 Exemptions of general applicability.

* * * * *

(b) * * *

(9) Technical data, including classified information, regardless of media or format, exported by or to a U.S. person or a foreign person employee of a U.S. person, travelling or on temporary assignment abroad subject to the following restrictions:

(i) Foreign persons may only export or receive such technical data as they are authorized to receive through a separate license or other approval.

(ii) The technical data exported under this authorization is to be possessed or used solely by a U.S. person or authorized foreign person and sufficient security precautions must be taken to prevent the unauthorized release of the technology. Such security precautions include encryption of the technical data, the use of secure network connections, such as virtual private networks, the use of passwords or other access restrictions on the electronic device or media on which the technical data is stored, and the use of firewalls and other network security measures to prevent unauthorized access.

(iii) The U.S. person is an employee of the U.S. government or is directly employed by a U.S. person and not by a foreign subsidiary.

(iv) Technical data authorized under this exception may not be used for foreign production purposes or for defense services unless authorized through a license or other approval.

(v) The U.S. employer of foreign persons must document the use of this exemption by foreign person employees,

including the reason that the technical data is needed by the foreign person for their temporary business activities abroad on behalf of the U.S. person.

(vi) Classified information is sent or taken outside the United States in accordance with the requirements of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case such guidance must be followed).

* * *

PART 127—VIOLATIONS AND PENALTIES

■ 22. The authority citation for part 127 continues to read as follows:

Authority: Sections 2, 38, and 42, 90, 90 Stat. 744 (22 U.S.C. 2752, 2778, 2791); 22 U.S.C. 401; 22 U.S.C. 2651a; 22 U.S.C. 2779a; 22 U.S.C. 2780; E.O. 13637, 78 FR 16129.

■ 23. Section 127.1 is amended by adding paragraphs (a)(6) and (b)(4) to read as follows:

§ 127.1 Violations.

(a) * * *

(6) To export, reexport, retransfer, or otherwise make available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in § 120.11(b) of this subchapter.

(b) * * *

(4) To release or otherwise transfer information, such as decryption keys, network access codes, or passwords, that would allow access to other technical data in clear text or to software that will result, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software. Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software.

* * *

Dated: May 20, 2015.

Rose E. Gottenmoeller,

Under Secretary, Arms Control and International Security, Department of State.

[FR Doc. 2015-12844 Filed 6-2-15; 8:45 am]

BILLING CODE 4710-25-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

24 CFR Parts 91 and 576

[Docket No. FR-5474-N-02]

RIN 2506-AC29

Emergency Solutions Grants (ESG) Program, Solicitation of Comment on Specific Issues

AGENCY: Office of the Assistant Secretary for Community Planning and Development, HUD.

ACTION: Regulatory review; request for comments.

SUMMARY: On December 5, 2011, HUD published an interim rule entitled "Homeless Emergency Assistance and Rapid Transition to Housing: Emergency Solutions Grants Program and Consolidated Plan Conforming Amendments" (interim rule). The comment period for the interim rule ended on February 3, 2012. Because recipients and subrecipients have now had more experience implementing the interim rule, HUD recognizes that they may have additional input and comments for HUD to consider in its development of the ESG final rule (final rule). Therefore, this document takes comments for 60 days to allow additional time for public input, and for HUD to solicit specific comment on certain issues.

DATES: *Comment due date:* August 3, 2015.

ADDRESSES: Interested persons are invited to submit comments responsive to this request for information to the Regulations Division, Office of General Counsel, Department of Housing and Urban Development, 451 7th Street SW., Room 10276, Washington, DC 20410-7000. Communications must refer to the above docket number and title and should contain the information specified in the "Request for Comments" of this notice.

Electronic Submission of Comments. Interested persons may submit comments electronically through the Federal eRulemaking Portal at <http://www.regulations.gov>. HUD strongly encourages commenters to submit comments electronically. Electronic submission of comments allows the commenter maximum time to prepare and submit a comment, ensures timely receipt by HUD, and enables HUD to make them immediately available to the public. Comments submitted electronically through the <http://www.regulations.gov> Web site can be viewed by interested members of the public. Commenters should follow

instructions provided on that site to submit comments electronically.

Submission of Hard Copy Comments. Comments may be submitted by mail or hand delivery. To ensure that the information is fully considered by all of the reviewers, each commenter submitting hard copy comments, by mail or hand delivery, should submit comments or requests to the address above, addressed to the attention of the Regulations Division. Due to security measures at all federal agencies, submission of comments or requests by mail often result in delayed delivery. To ensure timely receipt of comments, HUD recommends that any comments submitted by mail be submitted at least 2 weeks in advance of the public comment deadline. All hard copy comments received by mail or hand delivery are a part of the public record and will be posted to <http://www.regulations.gov> without change.

Note: To receive consideration as public comments, comments must be submitted through one of the two methods specified above. Again, all submissions must refer to the docket number and title of the rule.

No Facsimile Comments. Facsimile (fax) comments are not acceptable.

Public Inspection of Comments. All comments submitted to HUD regarding this notice will be available, without charge, for public inspection and copying between 8 a.m. and 5 p.m. weekdays at the above address. Due to security measures at the HUD Headquarters building, an advance appointment to review the documents must be scheduled by calling the Regulation Division at 202-708-3055 (this is not a toll-free number). Copies of all comments submitted will also be available for inspection and downloading at <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT:

Norm Suchar, Director, Office of Special Needs Assistance Programs, Office of Community Planning and Development, Department of Housing and Urban Development, 451 7th Street SW., Room 7262, Washington, DC 20410-7000, telephone number (202) 708-4300 (this is not a toll-free number). Persons with hearing or speech impairments may access this number through TTY by calling the toll-free Federal Relay Service at 800-877-8339.

SUPPLEMENTARY INFORMATION:

Exhibit 5



United States Department of State

*Bureau of Political-Military Affairs
Office of Defense Trade Controls Compliance
Washington, D.C. 20522-0112*

MAY 08 2013

In reply refer to

Mr. Cody Wilson
Defense Distributed

Dear Mr. Wilson:

The Department of State, Bureau of Political Military Affairs, Office of Defense Trade Controls Compliance, Enforcement Division (DTCC/END) is responsible for compliance with and civil enforcement of the Arms Export Control Act (22 U.S.C. 2778) (AECA) and the AECA's implementing regulations, the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130) (ITAR). The AECA and the ITAR impose certain requirements and restrictions on the transfer of, and access to, controlled defense articles and related technical data designated by the United States Munitions List (USML) (22 C.F.R. Part 121).

DTCC/END is conducting a review of technical data made publicly available by Defense Distributed through its 3D printing website, DEF CAD.org, the majority of which appear to be related to items in Category I of the USML. Defense Distributed may have released ITAR-controlled technical data without the required prior authorization from the Directorate of Defense Trade Controls (DDTC), a violation of the ITAR.

Technical data regulated under the ITAR refers to information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, including information in the form of blueprints, drawings, photographs, plans, instructions or documentation. For a complete definition of technical data, see § 120.10 of the ITAR. Pursuant to § 127.1 of the ITAR,

it is unlawful to export any defense article or technical data for which a license or written approval is required without first obtaining the required authorization from the DDTC. Please note that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is considered an export under § 120.17 of the ITAR.

The Department believes Defense Distributed may not have established the proper jurisdiction of the subject technical data. To resolve this matter officially, we request that Defense Distributed submit Commodity Jurisdiction (CJ) determination requests for the following selection of data files available on DEFCAD.org, and any other technical data for which Defense Distributed is unable to determine proper jurisdiction:

1. Defense Distributed Liberator pistol
2. .22 electric
3. 125mm BK-14M high-explosive anti-tank warhead
4. 5.56/.223 muzzle brake
5. Springfield XD-40 tactical slide assembly
6. Sound Moderator – slip on
7. “The Dirty Diane” 1/2-28 to 3/4-16 STP S3600 oil filter silencer adapter
8. 12 gauge to .22 CB sub-caliber insert
9. Voltlock electronic black powder system
10. VZ-58 front sight.

DTCC/END requests that Defense Distributed submit its CJ requests within three weeks of receipt of this letter and notify this office of the final CJ determinations. All CJ requests must be submitted electronically through an online application using the DS-4076 Commodity Jurisdiction Request Form. The form, guidance for submitting CJ requests, and other relevant information such as a copy of the ITAR can be found on DDTC’s website at <http://www.pmddtc.state.gov>.

Until the Department provides Defense Distributed with final CJ determinations, Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately. Defense Distributed should also review the remainder of the data made public on its website to

- 3 -

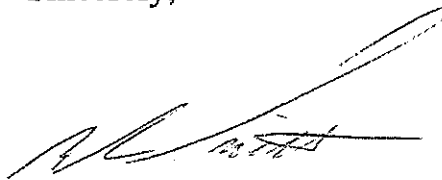
determine whether any additional data may be similarly controlled and proceed according to ITAR requirements.

Additionally, DTCC/END requests information about the procedures Defense Distributed follows to determine the classification of its technical data, to include the aforementioned technical data files. We ask that you provide your procedures for determining proper jurisdiction of technical data within 30 days of the date of this letter to Ms. Bridget Van Buren, Compliance Specialist, Enforcement Division, at the address below:

Office of Defense Trade Controls Compliance
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

We appreciate your full cooperation in this matter. Please note our reference number in any future correspondence.

Sincerely,



Glenn E. Smith
Chief, Enforcement Division

Exhibit 6

SETTLEMENT AGREEMENT

Defense Distributed (“DD”), Second Amendment Foundation, Inc. (“SAF”), and Conn Williamson (collectively, “Plaintiffs,”) and the United States Department of State (“State”), the Secretary of State, the Directorate of Defense Trade Controls (“DDTC”), the Deputy Assistant Secretary, Defense Trade Controls, and the Director, Office of Defense Trade Controls Policy (collectively, “Defendants”), out of a mutual desire to resolve all of the claims in the case captioned *Defense Distributed, et al. v. Dep’t of State, et al.*, Case No. 15-cv-372-RP (W.D. Tex.) (the “Action”) without the need for further litigation and without any admission of liability, hereby stipulate and agree as follows:

Plaintiffs and Defendants do hereby settle all claims, issues, complaints, or actions described in the case captioned, and any and all other claims, complaints, or issues that have been or could have been asserted by Plaintiffs against Defendants in accordance with the following terms and conditions:

1. *Consideration:* In consideration of Plaintiffs’ agreement to dismiss the claims in the Action with prejudice as described in paragraph 2, below, Defendants agree to the following, in accordance with the definitions set forth in paragraph 12, below:

- (a) Defendants’ commitment to draft and to fully pursue, to the extent authorized by law (including the Administrative Procedure Act), the publication in the Federal Register of a notice of proposed rulemaking and final rule, revising USML Category I to exclude the technical data that is the subject of the Action.
- (b) Defendants’ announcement, while the above-referenced final rule is in development, of a temporary modification, consistent with the International

Traffic in Arms Regulations (ITAR), 22 C.F.R. § 126.2, of USML Category I to exclude the technical data that is the subject of the Action. The announcement will appear on the DDTC website, www.pmddtc.state.gov, on or before July 27, 2018.

- (c) Defendants' issuance of a letter to Plaintiffs on or before July 27, 2018, signed by the Deputy Assistant Secretary for Defense Trade Controls, advising that the Published Files, Ghost Gunner Files, and CAD Files are approved for public release (i.e., unlimited distribution) in any form and are exempt from the export licensing requirements of the ITAR because they satisfy the criteria of 22 C.F.R. § 125.4(b)(13). For the purposes of 22 C.F.R. § 125.4(b)(13) the Department of State is the cognizant U.S. Government department or agency, and the Directorate of Defense Trade Controls has delegated authority to issue this approval.
- (d) Defendants' acknowledgment and agreement that the temporary modification of USML Category I permits any United States person, to include DD's customers and SAF's members, to access, discuss, use, reproduce, or otherwise benefit from the technical data that is the subject of the Action, and that the letter to Plaintiffs permits any such person to access, discuss, use, reproduce or otherwise benefit from the Published Files, Ghost Gunner Files, and CAD Files.
- (e) Payment in the amount of \$39,581.00. This figure is inclusive of any interest and is the only payment that will be made to Plaintiffs or their counsel by Defendants under this Settlement Agreement. Plaintiffs' counsel will provide Defendants'

counsel with all information necessary to effectuate this payment.

The items set forth in subparagraphs (a) through (e) above constitute all relief to be provided in settlement of the Action, including all damages or other monetary relief, equitable relief, declaratory relief, or relief of any form, including but not limited to, attorneys' fees, costs, and/or relief recoverable pursuant to 2 U.S.C. § 1302, 2 U.S.C. § 1311, 2 U.S.C. § 1317, 22 U.S.C. § 6432b(g), 28 U.S.C. § 1920, Fed. R. Civ. P. 54(d), and the Local Rules.

2. *Dismissal with Prejudice:* At the time of the execution of this Settlement Agreement, Plaintiffs agree to have their counsel execute and provide to Defendants' counsel an original Stipulation for Dismissal with Prejudice pursuant to Fed. R. Civ. P. 41(a)(1)(A)(ii) and 41(a)(1)(B). Counsel for Defendants agree to execute the stipulation and file it with the Court in the Action, no sooner than 5 business days after the publication of the announcement described in Paragraph 1(b) of this Settlement Agreement and issuance of the letter described in Paragraph 1(c) of this Settlement Agreement. A copy of the Stipulation for Dismissal with Prejudice is attached hereto.
3. *Release:* Plaintiffs, for themselves and their administrators, heirs, representatives, successors, or assigns, hereby waive, release and forever discharge Defendants, and all of their components, offices or establishments, and any officers, employees, agents, or successors of any such components, offices or establishments, either in their official or

individual capacities, from any and all claims, demands and causes of action of every kind, nature or description, whether currently known or unknown, which Plaintiffs may have had, may now have, or may hereafter discover that were or could have been raised in the Action.

4. *No Admission of Liability:* This Settlement Agreement is not and shall not be construed as an admission by Defendants of the truth of any allegation or the validity of any claim asserted in the Action, or of Defendants' liability therein. Nor is it a concession or an admission of any fault or omission in any act or failure to act. Nor is it a concession or admission as to whether the monetary or equitable relief, attorneys' fees, costs, and expenses sought by Plaintiffs in the Action, are reasonable or appropriate. None of the terms of the Settlement Agreement may be offered or received in evidence or in any way referred to in any civil, criminal, or administrative action other than proceedings permitted by law, if any, that may be necessary to consummate or enforce this Settlement Agreement. The terms of this Settlement Agreement shall not be construed as an admission by Defendants that the consideration to be given hereunder represents the relief that could be recovered after trial. Defendants deny that they engaged in *ultra vires* actions, deny that they violated the First Amendment, Second Amendment, or Fifth Amendment of the United States Constitution, and maintain that all of the actions taken by Defendants with respect to Plaintiffs comply fully with the law, including the United States Constitution.

5. *Merger Clause:* The terms of this Settlement Agreement constitute the entire agreement of Plaintiffs and Defendants entered into in good faith, and no statement, remark, agreement or understanding, oral or written, which is not contained therein, shall be recognized or enforced. Plaintiffs acknowledge and agree that no promise or representation not contained in this Settlement Agreement has been made to them and they acknowledge and represent that this Settlement Agreement contains the entire understanding between Plaintiffs and Defendants and contains all terms and conditions pertaining to the compromise and settlement of the disputes referenced herein. Nor does the Parties' agreement to this Settlement Agreement reflect any agreed-upon purpose other than the desire of the Parties to reach a full and final conclusion of the Action, and to resolve the Action without the time and expense of further litigation.
6. *Amendments:* This Settlement Agreement cannot be modified or amended except by an instrument in writing, agreed to and signed by the Parties, nor shall any provision hereof be waived other than by a written waiver, signed by the Parties.
7. *Binding Successors:* This Settlement Agreement shall be binding upon and inure to the benefit of Plaintiffs and Defendants, and their respective heirs, executors, successors, assigns and personal representatives, including any persons, entities, departments or agencies succeeding to the interests or obligations of the Parties.

8. *Consultation with Counsel:* Plaintiffs acknowledges that they have discussed this Settlement Agreement with their counsel, who has explained these documents to them and that they understand all of the terms and conditions of this Settlement Agreement. Plaintiffs further acknowledge that they have read this Settlement Agreement, understand the contents thereof, and execute this Settlement Agreement of their own free act and deed. The undersigned represent that they are fully authorized to enter into this Settlement Agreement.
9. *Execution:* This Settlement Agreement may be executed in one or more counterparts, each of which shall be deemed an original, and all of which together constitute one and the same instrument, and photographic copies of such signed counterparts may be used in lieu of the original.
10. *Jointly Drafted Agreement:* This Settlement Agreement shall be considered a jointly drafted agreement and shall not be construed against any party as the drafter.
11. *Tax and Other Consequences:* Compliance with all applicable federal, state, and local tax requirements shall be the sole responsibility of Plaintiffs and their counsel. Plaintiffs and Defendants agree that nothing in this Settlement Agreement waives or modifies federal, state, or local law pertaining to taxes, offsets, levies, and liens that may apply to this

Settlement Agreement or the settlement proceeds, and that Plaintiffs are executing this Settlement Agreement without reliance on any representation by Defendants as to the application of any such law.

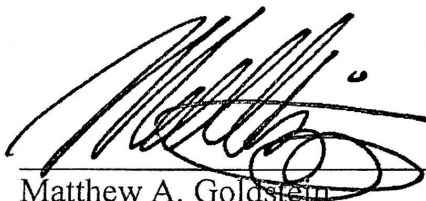
12. *Definitions:* As used in this Settlement Agreement, certain terms are defined as follows:

- The phrase “*Published Files*” means the files described in paragraph 25 of Plaintiffs’ Second Amended Complaint.
- The phrase “*Ghost Gunner Files*” means the files described in paragraph 36 of Plaintiffs’ Second Amended Complaint.
- The phrase “*CAD Files*” means the files described in paragraph 40 of Plaintiffs’ Second Amended Complaint.
- The phrase “*Other Files*” means the files described in paragraphs 44-45 of Plaintiffs’ Second Amended Complaint.
- The phrase “*Military Equipment*” means (1) Drum and other magazines for firearms to .50 caliber (12.7 mm) inclusive with a capacity greater than 50 rounds, regardless of jurisdiction of the firearm, and specially designed parts and components therefor; (2) Parts and components specially designed for conversion of a semi-automatic firearm to a fully automatic firearm; (3) Accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting, and specially designed parts and components therefor.
- The phrase “*technical data that is the subject of the Action*” means: (1) the Published Files; (2) the Ghost Gunner Files; (3) the CAD Files; and (4) the Other Files insofar as those files regard items exclusively: (a) in Category I(a) of the United States Munitions List (USML), as well as barrels and receivers covered by Category I(g) of the USML that are components of such items; or (b) items.

covered by Category I(h) of the USML solely by reference to Category I(a),
excluding Military Equipment.

Dated: June 29, 2018

Dated: June 29, 2018



Matthew A. Goldstein
Snell & Wilmer LLP
One South Church Ave. Ste. 1500
Tucson, Arizona 85701
Counsel for Plaintiffs

Dated: June 29, 2018



Eric J. Soskin
Stuart J. Robinson
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W.
Washington, D.C. 20001
Tel. (202) 353-0533

Counsel for Defendants

Exhibit 7

① NOTICE: GENERAL

07/27/18

Temporary Modification of Category I of the United States Munitions List

Consistent with the International Traffic in Arms Regulations (ITAR), 22 C.F.R. § 126.2, the Acting Deputy Assistant Secretary for Defense Trade Controls has determined that it is in the interest of the security and foreign policy of the United States to temporarily modify United States Munitions List (USML) Category I to exclude the following technical data identified in the Settlement Agreement for the matter of *Defense Distributed, et al., v. U.S. Department of State, et al*, Case No. 15-cv-372-RP (W.D. Tex.) (hereinafter "*Defense Distributed*"):

- "Published Files," i.e., the files described in paragraph 25 of the Second Amended Complaint in *Defense Distributed*.
- "Ghost Gunner Files," i.e., the files described in paragraph 36 of the Second Amended Complaint in *Defense Distributed*.
- "CAD Files," i.e., the files described in paragraph 40 of the Second Amended Complaint in *Defense Distributed*.
- "Other Files," i.e., the files described in paragraphs 44-45 of the Second Amended Complaint in *Defense Distributed*, insofar as those files regard items exclusively: (a) in Category I(a) of the USML, as well as barrels and receivers covered by Category I(g) of the USML that are components of such items; or (b) items covered by Category I(h) of the USML solely by reference to Category I(a), excluding Military Equipment. Military Equipment means (1) Drum and other magazines for firearms to .50 caliber (12.7 mm) inclusive with a capacity greater than 50 rounds, regardless of jurisdiction of the firearm, and specially designed parts and components therefor; (2) Parts and components specially designed for conversion of a semi-automatic firearm to a fully automatic firearm; (3) Accessories or attachments specially designed to automatically stabilize aim (other than gun rests) or for automatic targeting, and specially designed parts and components therefor.

This temporary modification will remain in effect while the final rule referenced in paragraph 1(a) of the Settlement Agreement is in development.

Please see the [Settlement Agreement](#) and the [Second Amended Complaint](#) for additional information.

Exhibit 8



(/)

Engel Decries State Department Policy to Allow 3-D Gun Printing

Jul 20, 2018 | Press Release

WASHINGTON—Rep. Eliot L. Engel, Ranking Member of the House Committee on Foreign Affairs, today called on Secretary of State Mike Pompeo to immediately suspend a dangerous State Department policy which would permit internet publication of software for 3-D gun printing.

“There are several disturbing aspects of the Department’s action. Foremost is the likelihood that weapons will become available to anyone with a laptop and a 3-D printer. This defeats US laws which require background checks on the sale of weaponry. The danger is magnified because 3-D printed firearms would be made of plastic and, therefore, undetectable by most security systems. With these stealthy weapons in the hands of terrorists, lone wolf killers, or mentally unstable individuals, it will become virtually impossible to protect anyone from gun violence,” Ranking Member Engel wrote.

The State Department’s change in policy is the result of a settlement of a law suit: Defense Distributed v. United States. If no action is taken, the policy takes effect on July 27, 2018.

Text of the letter can be found here (<https://democrats-foreignaffairs.house.gov/sites/democrats.foreignaffairs.house.gov/files/07-20-18%20Letter%20to%20Secretary%20Pompeo%20Regarding%203-D%20Printed%20Arms.pdf>) and below:

Dear Mr. Secretary:

I write to register my profound concern about an action by Department of State officials to remove from export controls certain software for 3-D printing of firearms. This is exceptionally dangerous because it will promote global availability of such technical information and consequent unrestricted manufacture of firearms. This action was taken in settling a lawsuit: Defense Distributed v. United States.

There are several disturbing aspects of the Department’s action. Foremost is the likelihood that weapons will become available to anyone with a laptop and a 3-D printer. This defeats US laws which require background checks on the sale of weaponry. The danger is magnified because 3-D printed firearms would be made of

plastic and, therefore, undetectable by most security systems. With these stealthy weapons in the hands of terrorists, lone wolf killers, or mentally unstable individuals, it will become virtually impossible to protect anyone from gun violence.

Moreover, the text of the settlement, attached, suggests that the Department's officials are mis-using authority under Section 126.2 of the International Traffic in Arms Regulations to "temporarily" remove this technical information from the United States Munitions List (USML). However, as anyone who has ever posted something on the internet knows, once posted, the item is instantly and permanently available to all who seek it. Therefore, it is impossible to temporarily publish 3-D gun printing software on the internet. In as much as Sec. 126.2's authority is reserved for use only in the interests of U.S. security and foreign policy. It stretches credulity to believe that release of this information is in the U.S. interest.

Use of this temporary ITAR authority also suggests that Department officials sought a way to avoid complying with Section 38(f) of the Arms Export Control Act, which requires advance notification to Congress for any removal from the USML.

The settlement of this lawsuit is slated to go into effect by July 27th. I urge you to suspend the Department's implementation of the settlement immediately and prevent the inappropriate and dangerous release of this technical information.

Sincerely,

#